EDITRAN/GC

Gestión de claves

Windows

Manual de Usuario

INDRA
30 de octubre de 2014

1. INTRODUCCIÓN. 1-1

2. ORGANIZACIÓN DE LA INTERFAZ GRÁFICA 2-1

2.1. Árbol de selección de tipos de Subsistemas 2-2

2.2. Lista o Listas de Subsistemas 2-2

2.3. Barra de Herramientas 2-3
2.3.1. Nuevo Subsistema 2-3
2.3.2. Modificar Subsistemas 2-4
2.3.3. Eliminar Subsistemas 2-4
2.3.4. Generar Fichero de Envío 2-4
2.3.5. Actualizar la clave de un Subsistema Local RSA 2-4
2.3.6. Generar una nueva clave y Fichero DES 2-4
2.3.7. Insertar Fichero Remoto 2-5
2.3.8. Crear nueva clave Propia 2-5
2.3.9. Mostrar Claves Propias RSA 2-5
2.3.10. Modificar una Clave Propia 2-6
2.3.11. Eliminar una Clave Propia 2-6
2.3.12. Generar una nueva Versión de la Clave 2-6
2.3.13. Actualización y Refresco de los datos 2-6

3. INTERCAMBIO DE CLAVES RSA. 3-1

3.1. Generación y Envío de una Clave Local RSA 3-1
3.1.1. Clave Local RSA 3-1
3.1.1.1. Creación de una Clave Propia RSA 3-2
3.1.1.2. Modificación, Consulta y Eliminación de una Clave Propia 3-3
3.1.1.3. Consulta de la clave pública generada 3-4
3.1.1.4. Generación de nueva versión de una Claves RSA 3-4
3.1.1.5. Asociación de Claves a Remotos 3-5
3.1.2. Subsistema Local RSA 3-7
3.1.2.1. Producción del fichero de intercambio 3-7
3.1.2.2. Envío del fichero al remoto 3-8
3.1.2.3. Actualización de claves del subsistema 3-11
3.1.2.4. Versión de la Clave en vuelo 3-11
3.1.2.5. Inserción de un fichero de confirmación 3-11

3.2. Generación de un Subsistema Remoto RSA y envío de la confirmación 3-12
3.2.1. Generación de un Subsistema Remoto RSA 3-12
3.2.2. Incorporación de un fichero de intercambio remoto 3-13
3.2.3. Generación y envío de la confirmación 3-14

3.3. Otras operaciones comunes sobre los subsistemas 3-15
3.3.1. Modificación, Consulta y Eliminación de un subsistema Local RSA 3-15
3.3.2. Consulta de claves RSA 3-16
3.3.3. Modificación manual del estado de una clave RSA 3-16
3.3.4. Activación y Cancelación de una clave RSA 3-17

4. INTERCAMBIO DE CLAVES DES 4-1

4.1. Subsistema Local DES 4-1
4.1.1. Creación de un subsistema Local DES 4-2
4.1.1.1. Requisitos previos 4-2
4.1.1.2. Creación del subsistema 4-2
4.1.1.3. Envío del fichero de intercambio al remoto utilizando EDItran 4-3
4.1.2. Generación de nuevas versiones de claves DES 4-5
4.1.3. Inserción de un fichero de confirmación 4-6

4.2. Creación de Subsistema Remoto DES 4-6
4.2.1. Creación de un subsistema Remoto DES 4-6
4.2.2. Incorporación de un fichero de intercambio remoto 4-7
4.2.3. Generación y envío de la confirmación 4-9

4.3. Otras operaciones comunes de subsistemas DES 4-10
4.3.1. Modificación, Consulta y Eliminación de un subsistema DES 4-10
4.3.2. Consulta de claves DES 4-11
4.3.3. Modificación manual del estado de una clave DES 4-11
4.3.4. Activación y Cancelación de una clave DES 4-12

5. UTILIZACIÓN DE EDITRAN JUNTO A EDITRAN/GC 5-1

5.1. Envío y recepción automática utilizando EDItran 5-1

5.1.1. Subsistema Local 5-1
5.1.2. Subsistema Remoto 5-1
5.1.3. Perfiles de EDItran/G 5-2

5.2. Procedimiento Automático para EDItran 5-2
5.2.1. PSTRECGC.bat 5-3

6. APENDICES 6-1

6.1. Estados de los subsistemas 6-1

6.2. Diagrama de Estados 6-2
6.2.1. Clave Propia RSA 6-2
6.2.2. Clave Local 6-2
6.2.3. Clave Remota 6-3

1. Introducción.

EDItran facilita al usuario la posibilidad de utilizar varias formas de intercambiar datos protegidos mediante las siguientes modalidades de criptografía:

Modalidad 2.2. Criptografía con autenticación y confidencialidad con algoritmo DES de claves simples de 8 bytes. El intercambio de claves se realiza de manera automática.

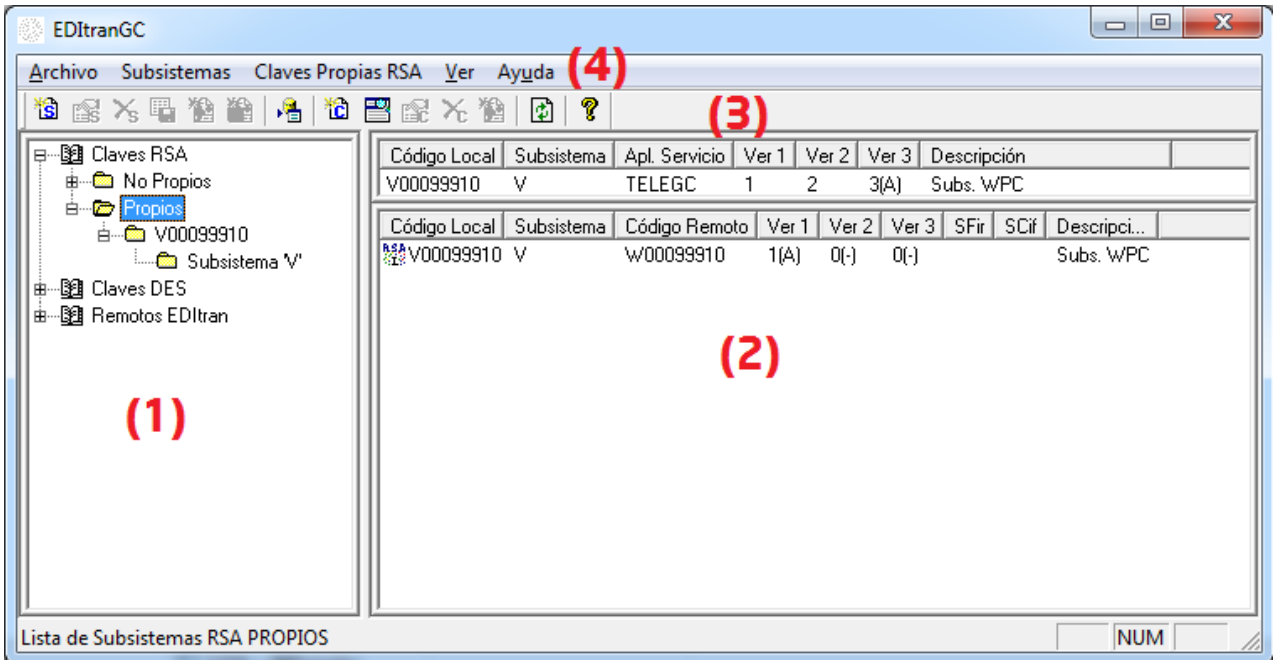
Modalidad 3.0. Criptografía de autenticación con algoritmo DES, TDES, RSA y Certificados Digitales (PKI) y con confidencialidad DES de claves simples, dobles o triples.

En la modalidad 3.0, excepto en el caso de autenticación PKI, las claves han de intercambiarse entre los extremos antes de poder utilizarlas.

2. Organización de la Interfaz gráfica

La interfaz gráfica está dividida en varios componentes claramente identificados:

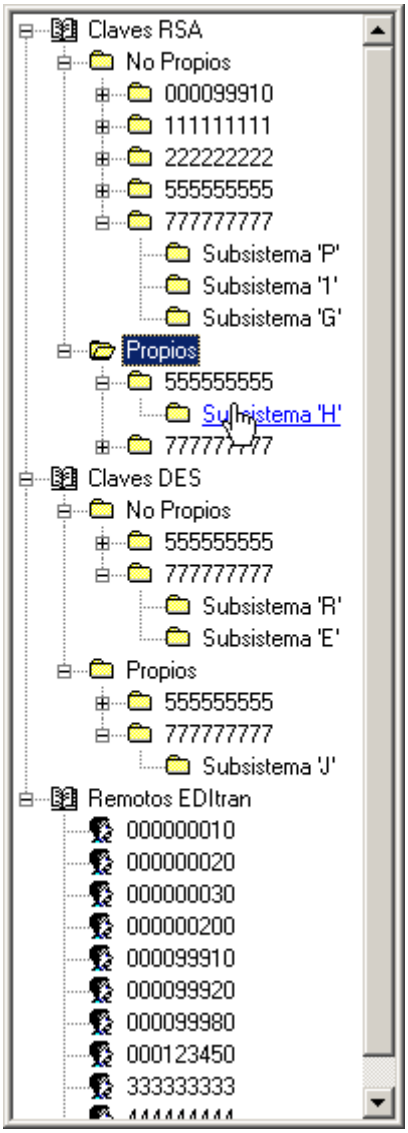
- (1) Árbol de selección de tipos de Subsistemas
- (2) Lista o Listas de Subsistemas
- (3) Barra de Herramientas
- (4) Menú



Según se va desplegando las ramas del árbol (1) se va actualizando el contenido de la lista (3) con los subsistemas correspondientes. Seleccionando un subsistema de la lista y pinchándolo con el botón derecho del menú aparecen las opciones que se pueden efectuar sobre el subsistema.

A continuación detallaremos cada componente de la interfaz.

2.1. Árbol de selección de tipos de Subsistemas



El árbol contiene unas ramas 'fijas' que siempre existen y otras ramas variables que están inmediatamente por debajo de éstas y que dependen de los subsistemas que estén dados de alta.

Las ramas 'fijas' tienen la siguiente apariencia:

- ***Claves RSA*** (Muestra todos los subsistemas RSA)
  - ***No Propio*** (Muestra subsistemas Remotos RSA)
  - ***Propios*** (Muestra subsistemas Locales RSA)
- ***Claves DES*** (Muestra todos los subsistemas DES)
  - ***No Propios*** (Muestra subsistemas Remotos DES)
  - ***Propios*** (Muestra subsistemas Locales DES)
- ***Remotos*** (Muestra los remotos dados de alta en EDItran/G y los subsistemas asociados a cada remoto.

Por ejemplo, si pinchamos sobre ***Clave DES***, automáticamente la lista de subsistemas se actualiza para mostrar todos los subsistemas DES. Si debajo de DES pinchamos ***Propios*** aparecen los entornos locales que tenemos dados de alta con subsistemas locales. Pinchando sobre un subsistema veremos en la lista el remoto asociado.

2.2. Lista o Listas de Subsistemas

En esta parte de la interfaz aparece una lista con los subsistemas que cumplen los requisitos seleccionados en el árbol, excepto cuando se seleccionan Claves Propias RSA.

En ese caso aparecen dos listas en vez de una. La lista de la parte superior muestra las Claves Propias, es decir claves que aún no se han asignado a remotos (ver sección 3.1) y la lista de la parte inferior los subsistemas locales RSA, es decir las claves que ya han sido asignadas a remotos (ver sección **0**

Subsistema Local RSA).

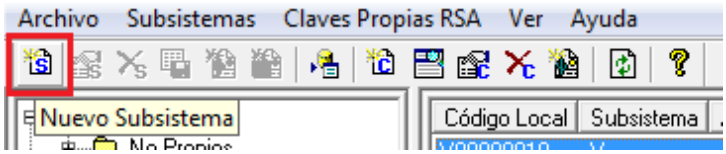
2.3. Barra de Herramientas

La barra de herramientas contiene botones que realizan prácticamente todas las operaciones que se pueden realizar sobre los subsistemas:

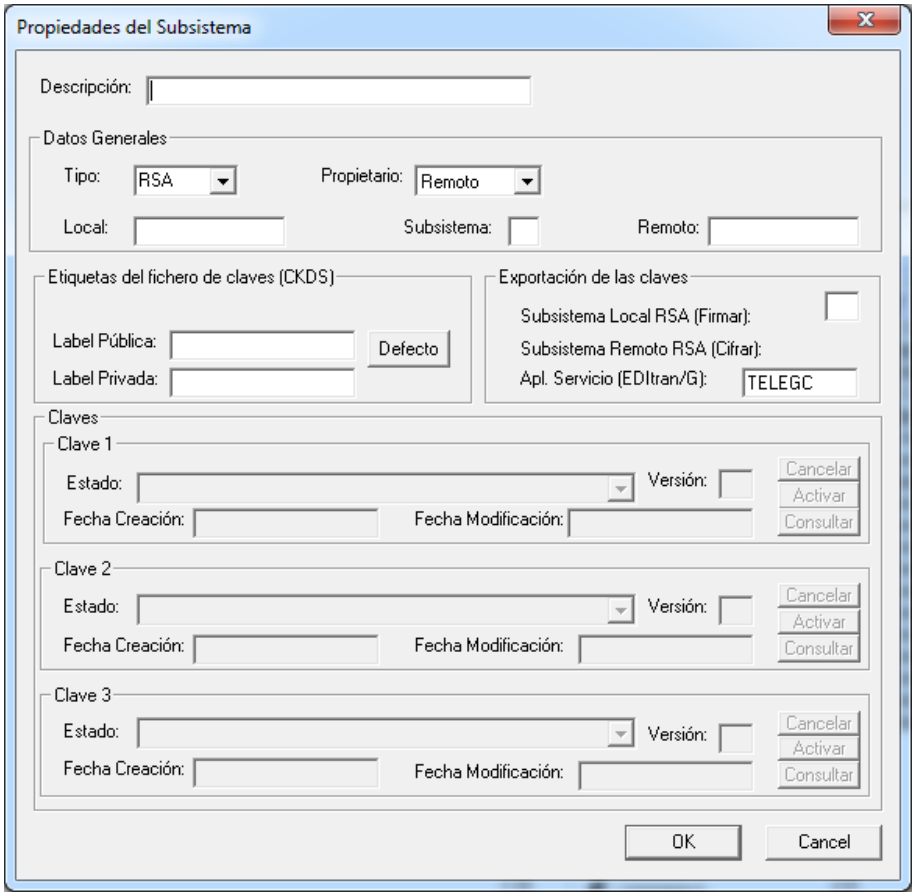
Dependiendo de la selección del árbol y del subsistema de la lista, algunos de los botones aparecerán desactivados.

A continuación se describirá brevemente la funcionalidad de cada uno de los botones de la barra de herramientas y se indicará el apartado donde se detalla en profundidad el efecto que se desencadena.

2.3.1. Nuevo Subsistema

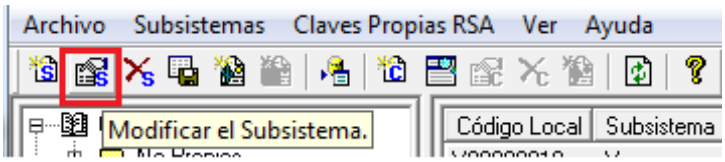


Se utiliza para crear un nuevo Subsistema. Al pulsar sobre el botón aparece el dialogo de nuevo subsistema:



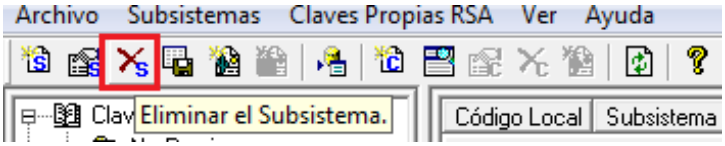
Podremos crear subsistemas DES Locales, DES Remotos y RSA Remotos. Los subsistemas RSA Locales deben crearse mediante la asociación de un Remoto a una Clave Propia (ver aparatado **3.1.1.5 Asociación de Claves a Remotos**).

2.3.2. Modificar Subsistemas



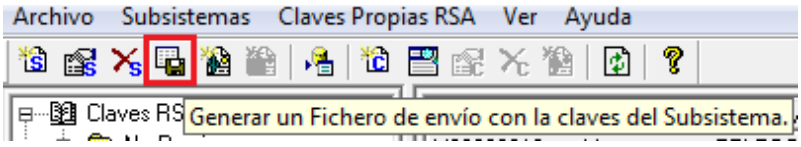
Al pinchar aparece el dialogo de las *Propiedades del Subsistema* (ver apartado 3.3.1) seleccionado en la lista.

2.3.3. Eliminar Subsistemas



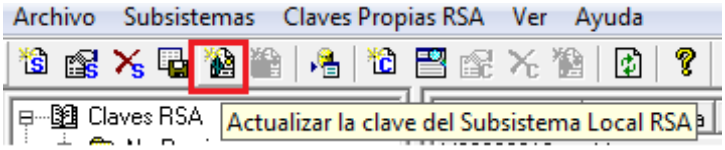
El botón está activo sólo cuando se selecciona un Subsistema. Al pinchar se eliminará, previa confirmación, el subsistema seleccionado en la lista.

2.3.4. Generar Fichero de Envío



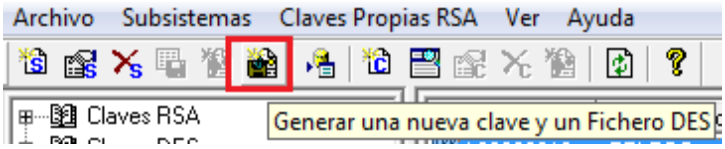
El botón está activo sólo cuando se selecciona un Subsistema Local RSA. Al pinchar genera un fichero de intercambio con la clave que se acabe de generar (en estado ***Generada***) y si se tiene dada de alta la Aplicación de Editran/G, se enviará automáticamente por EDItran (ver apartado 3.1.2.1).

2.3.5. Actualizar la clave de un Subsistema Local RSA



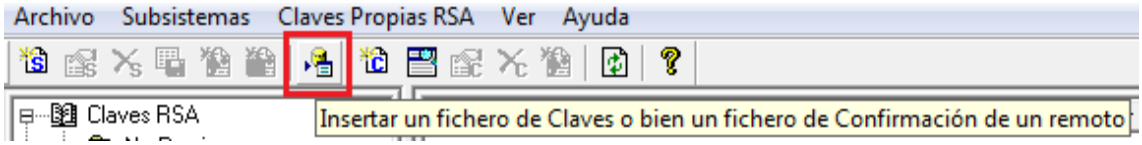
El botón está activo sólo cuando se selecciona un Subsistema Local RSA. Al pinchar se actualizará la clave del subsistema con la versión activa de la Clave Propia asociada (ver apartado **3.1.2.3 Actualización de claves del subsistema**).

2.3.6. Generar una nueva clave y Fichero DES

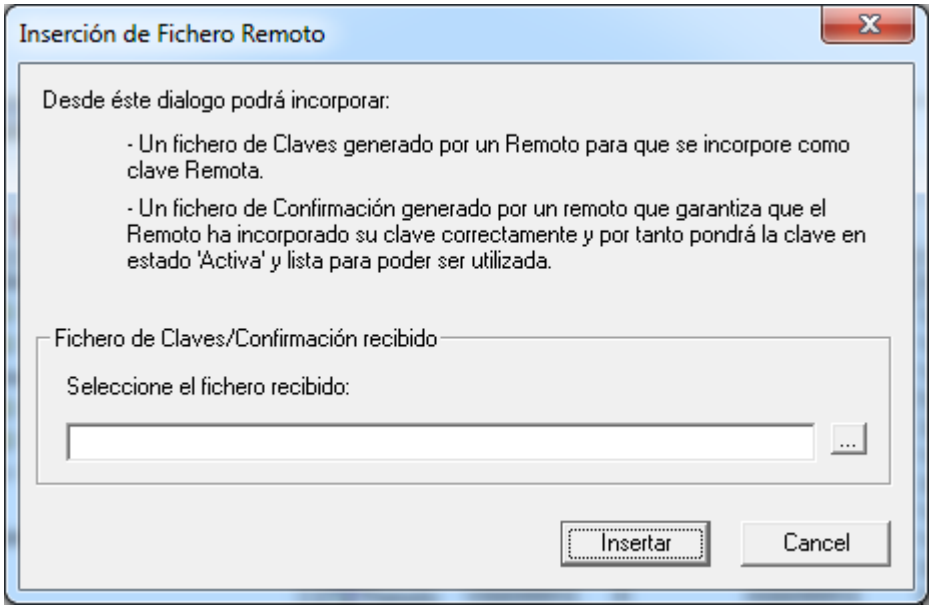


El botón está activo sólo cuando se selecciona un Subsistema Local DES. Al pinchar se generará una clave DES y un fichero de intercambio donde se almacena la clave DES cifrada y firmada utilizando subsistemas RSA. Para más información consultar el aparatado XXXXXXXXXXX.

2.3.7. Insertar Fichero Remoto


Archivo Subsistemas Claves Propias RSA Ver Ayuda
Claves RSA
Insertar un fichero de Claves o bien un fichero de Confirmación de un remoto

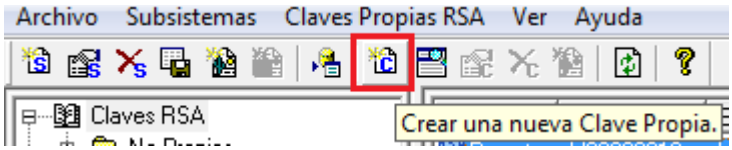
Al pinchar sobre el botón aparece un dialogo donde se indica el fichero que se quiere incorporar:


Inserción de Fichero Remoto
Desde éste dialogo podrá incorporar:
- Un fichero de Claves generado por un Remoto para que se incorpore como clave Remota.
- Un fichero de Confirmación generado por un remoto que garantiza que el Remoto ha incorporado su clave correctamente y por tanto pondrá la clave en estado 'Activa' y lista para poder ser utilizada.
Fichero de Claves/Confirmación recibido
Seleccione el fichero recibido:
...
Insertar
Cancel

El fichero, recibido de un remoto, podrá ser:

- Una clave pública RSA de un Remoto. Mas información en el apartado XXXXXX
- Una clave DES de un Remoto. Mas información en el apartado XXXXXX
- Una confirmación procedente de la incorporación de una clave DES/RSA en un remoto. Mas información en el apartado XXXXXX

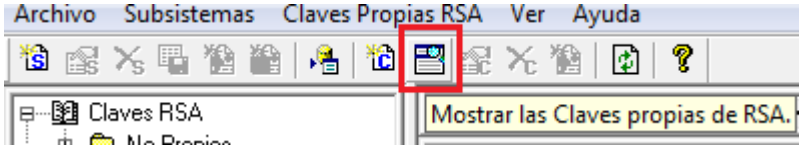
2.3.8. Crear nueva clave Propia



El botón está activo sólo cuando se selecciona una Clave Propia. Al pinchar se muestra el dialogo de Nueva Clave Propia. Para más información consultar el aparatado **0**

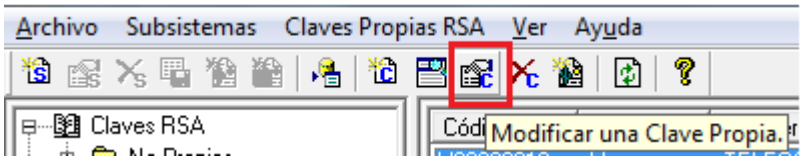
Creación de una Clave Propia RSA).

2.3.9. Mostrar Claves Propias RSA



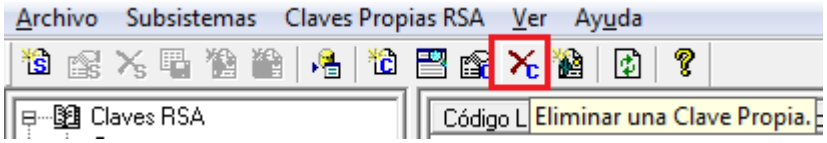
Al pinchar sobre el botón, la selección del árbol se coloca automáticamente en la Claves Propias RSA. De ésta manera podemos ver en la lista superior las Claves Propias y en la lista inferior los subsistemas Locales RSA.

2.3.10.Modificar una Clave Propia



El botón está activo sólo cuando se selecciona una Clave Propia. Al pinchar se muestra el dialogo de Propiedades de la Clave propia. Para más información consultar el apartado **3.1.1.2 Modificación, Consulta y Eliminación de una Clave Propia**.

2.3.11.Eliminar una Clave Propia



El botón está activo sólo cuando se selecciona una Clave Propia. Al pinchar se eliminará, previa confirmación, una Clave Propia RSA. Si existen subsistemas Locales RSA asociados a esa Clave Propia, la Clave Propia no podrá ser eliminada.

2.3.12.Generar una nueva Versión de la Clave

El botón está activo sólo cuando se selecciona una Clave Propia. Al pinchar se generarán un par de claves RSA y se aumentará la versión almacenada en la Clave Propia. Para más información consultar el aparatado **3.1.1.4 Generación de nueva versión de una Claves RSA**.

2.3.13.Actualización y Refresco de los datos

Archivo Subsistemas Claves Propias RSA Ver Ayuda
Claves RSA
Código Local
Refresca toda la información del arbol y las listas

Pinchando sobre el botón se refrescará toda la información del árbol y de la/las lista/s.

3. Intercambio de claves RSA.

Las claves RSA son claves criptográficas asimétricas. La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas.

Actualmente la Criptografía asimétrica es muy usada, sus dos principales aplicaciones son el intercambio de claves simétricas y la firma digital.

En este apartado se verá la forma de intercambiar una clave pública RSA con un remoto y la forma de insertar un fichero de intercambio generada por otro remoto utilizando EDItran/G.

3.1. Generación y Envío de una Clave Local RSA

Las claves RSA, por ser claves asimétricas, pueden ser intercambiadas con diferentes remotos sin peligro, ya que lo que se intercambia es la clave pública. La clave privada permanece únicamente en el sistema donde se ha creado y así no hay posibilidad de que los datos puedan ser descifrados por un tercero.

Por este motivo existen las ***Claves Propias RSA*** de EDItran/G. Mediante las Claves Propias RSA se administran una serie de funcionalidades comunes a todos los remotos que utilicen esa clave como son:

- Generación de nuevas versiones de la clave (nuevos pares de claves pública-privada)
- Activación de una u otra versión.
- Administración del Código Local y Subsistema.
- ...

Una Clave propia no puede utilizarse si no se ha intercambiado con un remoto. Para eso existe la posibilidad de asociar una Clave Propia a un Remoto, creando un ***Subsistema Local RSA***. Una vez asociado se podrá generar el fichero de intercambio y enviarlo al remoto para que éste incorpore nuestra clave pública.

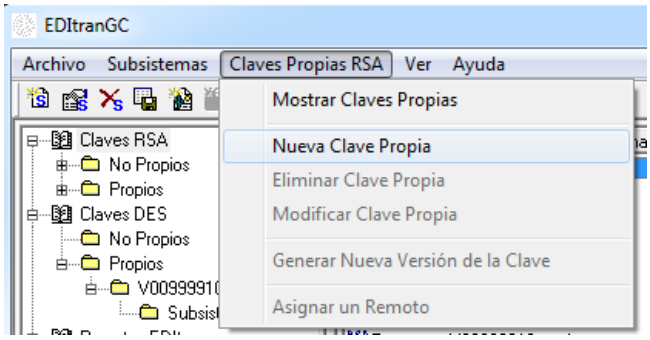
A continuación se describirá en detalle todos los pasos necesario para generar y enviar una clave RSA.

3.1.1. Clave Local RSA

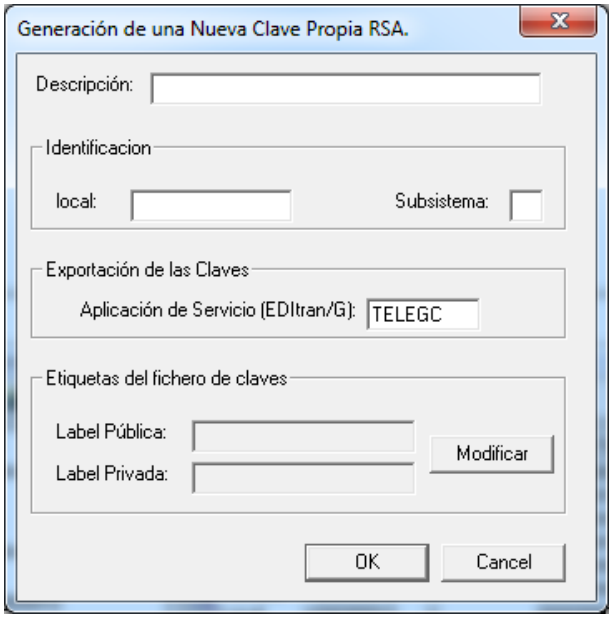
Como se apuntó en la sección anterior, una Clave Local RSA sirve para poder administrar funcionalidades independientes de los remotos y para poder generar nuevas claves RSA.

3.1.1.1.Creación de una Clave Propia RSA

Para crear una nueva Clave Local se utiliza el menú *Claves Propias RSA/Nueva Clave Propia*:



Aparece en dialogo de configuración de **Nueva Clave Propia**:



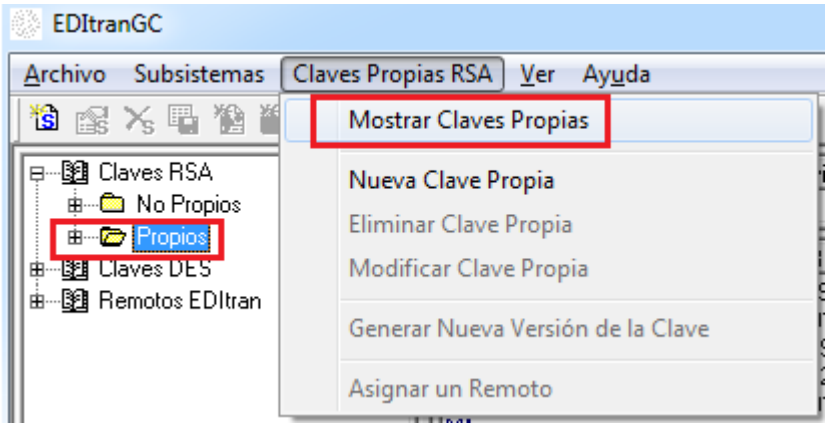
Los campos que aparecen son:

- **Descripción**: Es un campo meramente informativo.
- **Local**: Deberá poner el Entorno Local asignado a EDItran.
- **Subsistema**: Identificación de un solo carácter del tipo de clave. Para cada Entorno Local, puede tener diferentes subsistemas para lograr una operativa más sencilla (Subsistema de pruebas, subsistema real ...)
- **Aplicación de Servicio**: Aplicación de EDItran/G que se utilizará para enviar el fichero de intercambio. Se recomienda utilizar la Aplicación 'TELEGC'.
- **Label Pública**: Etiqueta con la que se almacenará la clave pública en el fichero *ckds.rsa*. Se recomienda no Modificar este valor si no se conoce en profundidad los problemas que pueden aparecer.
- **Label Privada**: Etiqueta con la que se almacenará la clave privada en el fichero *ckds.rsa*. Se recomienda no Modificar este valor si no se conoce en profundidad los problemas que pueden aparecer.

Una vez rellenados todos los campos pulsando OK se creará automáticamente un par de claves pública-privada que será la versión 1 de la Clave Local recientemente configurada.

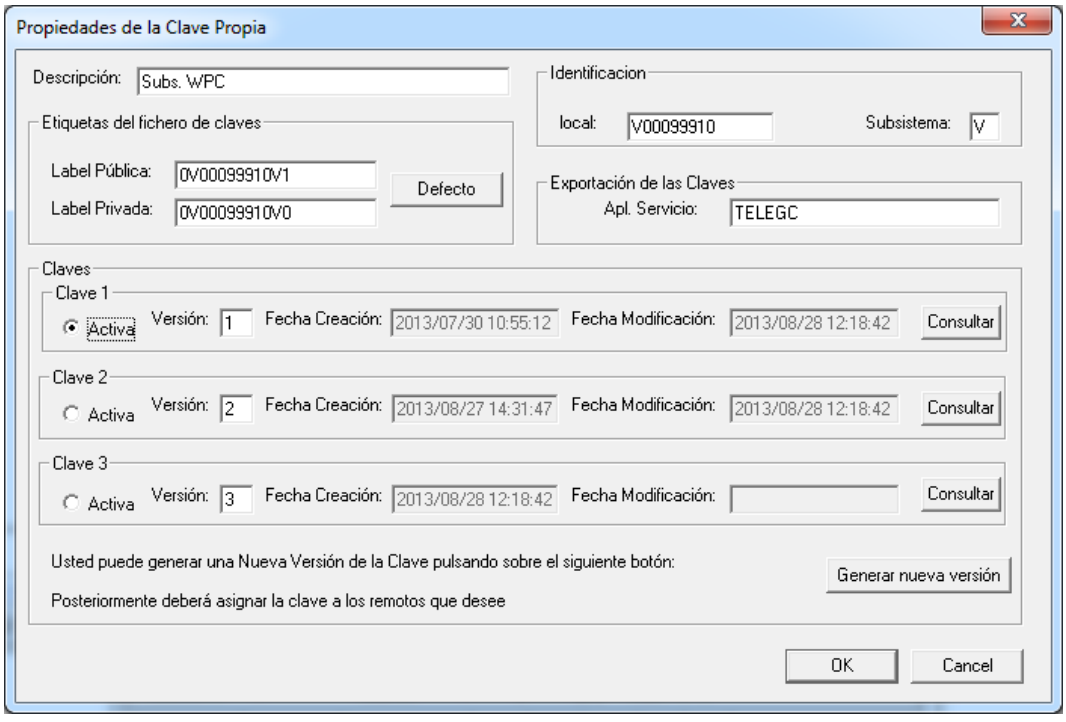
3.1.1.2.Modificación, Consulta y Eliminación de una Clave Propia

Para Consultar o modificar una clave propia primero debemos posicionarnos de modo que veamos la lista de claves propias, sencillamente pinchando en el árbol *Claves RSA/Propios* o mediante el menú *Claves Propias RSA/Mostrar Claves Propias:*



Veremos dos listas. La superior que contiene las Claves Propias RSA y la inferior los Subsistemas Locales RSA (Las Claves Propias asociadas a un Remoto).

Haciendo doble clic sobre la Clave Propia que deseemos Modificar/Consultar aparecerá el diálogo de propiedades de la Clave Propia con los datos que dimos de alta anteriormente (ver apartado **0 Creación de una Clave Propia RSA**), además de información de la clave RSA generada y diferentes botones para consultar la clave pública generada y generar una nueva versión de la clave:



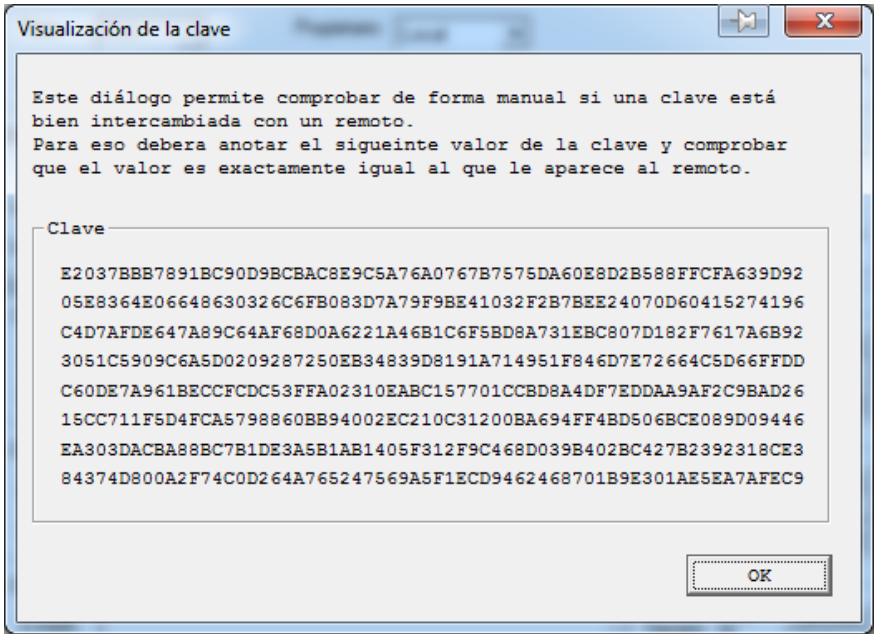
Desde éste dialogo se pueden modificar los parámetros que dimos previamente en el alta de la Clave Propia. No se recomiendan modificar ninguno de los parámetros dados de alta anteriormente. El único parámetro modificable es la Aplicación de servicio aunque es recomendable utilizar la Aplicación de EDItran/G 'TELEGC'.

También, desde el mismo dialogo se pueden realizar las siguientes operaciones sobre la clave pública:

- Consultar la clave pública generada (apartado 3.1.1.3)
- Generar una nueva pareja de claves RAS que constituirá una nueva versión de la Clave Propia (apartado 3.1.1.4)

3.1.1.3.Consulta de la clave pública generada

Al pulsar sobre el botón *Consultar* de una versión del dialogo de la Clave Propia veremos su clave pública:

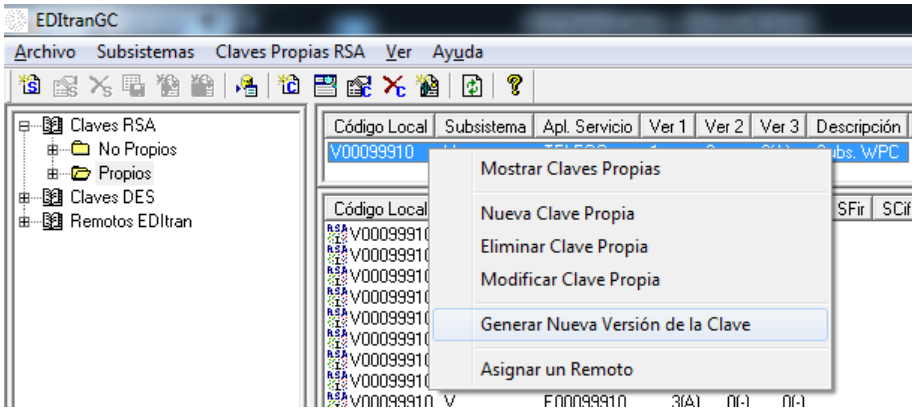

Visualización de la clave
Este diálogo permite comprobar de forma manual si una clave está bien intercambiada con un remoto.
Para eso debera anotar el sigueinte valor de la clave y comprobar que el valor es exactamente igual al que le aparece al remoto.
Clave
E2037BBB7891BC90D9BCBAC8E9C5A76A0767B7575DA60E8D2B588FFCFA639D92
05E8364E06648630326C6FB083D7A79F9BE41032F2B7BEE24070D60415274196
C4D7AFDE647A89C64AF68D0A6221A46B1C6F5BD8A731EBC807D182F7617A6B92
3051C5909C6A5D0209287250EB34839D8191A714951F846D7E72664C5D66FFDD
C60DE7A961BECCFCDC53FFA02310EABC157701CCBD8A4DF7EDDAA9AF2C9BAD26
15CC711F5D4FCA5798860BB94002EC210C31200BA694FF4BD506BCE089D09446
EA303DACBA88BC7B1DE3A5B1AB1405F312F9C468D039B402BC427B2392318CE3
84374D800A2F74C0D264A765247569A5F1ECD9462468701B9E301AE5EA7AFEC9
OK

Esta funcionalidad es útil para comparar la clave local propia, que hemos generado y permanece en nuestro sistema, con la Clave Remota RSA que el remoto habrá insertado en su sistema, incorporando el fichero de intercambio que habremos generado.

3.1.1.4.Generación de nueva versión de una Claves RSA

Existen tres maneras de generar una nueva versión de una Clave RSA:

- Pulsando sobre el botón *Generar Nueva Versión* del dialogo de consulta de la Clave Propia (3.1.1.2)
- Seleccionando el menú: *Claves propias/Generar Nueva Versión de la Clave* después de seleccionar la clave propia en la lista.
- Pulsando el botón de la derecha sobre la Clave Propia de la que deseamos generar una nueva versión y seleccionar *Generar Nueva Versión de la Clave*.:



Tras confirmar que se desea generar una nueva versión, se inicia un proceso de creación de una nueva pareja de claves RSA. Se le asignará una nueva versión a la nueva pareja de claves y nos mostrará la versión que se le ha sido asignada.

Ahora podremos comprobar que existen dos versiones:

Código Local	Subsistema	Apl. Servicio	Ver 1	Ver 2	Ver 3	Descripción
V00099910	V	TELEGC	1	2	3(A)	Subs. WPC

Se pueden almacenar hasta tres versiones de una clave y la lista muestra las versiones que se están almacenando en ese momento. Vemos que en la primera clave se almacena la versión 1 y que en la segunda la versión 2. Además vemos una 'A' entre paréntesis esto nos indica que la versión 2 es la versión activa.

❑ **Versión Activa de una Clave Propia**

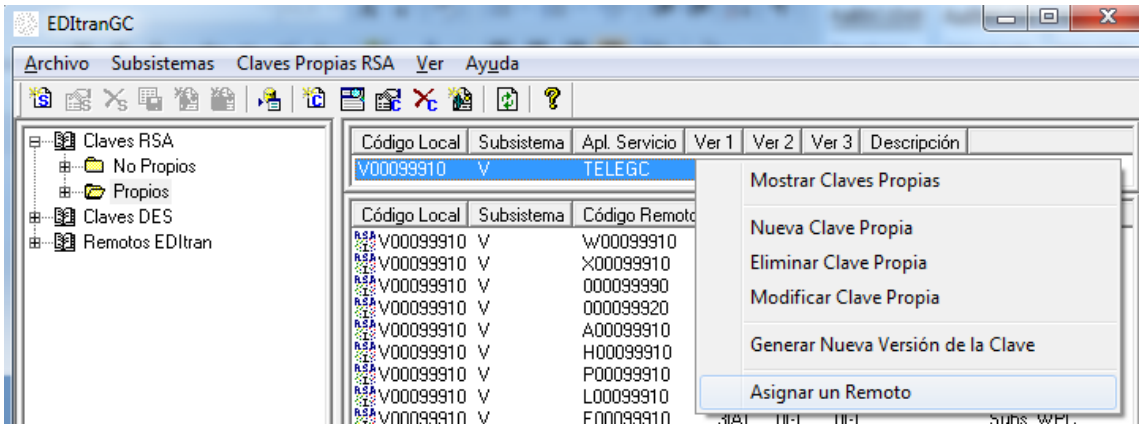
Una clave propia puede almacenar hasta tres versiones (tres parejas de claves RSA), sin embargo sólo una de ellas puede estar activa. La versión que está activa es la versión que se exportará al asociar la clave a un remoto (apartado 3.1.1.5). Al activar una clave, las otras dos (si existen) se desactivaran automáticamente.

Para activar una clave, desde el dialogo de Administración de la clave propia (apartado **3.1.1.2 Modificación, Consulta y Eliminación de una Clave Propia**) pinchar sobre el *Botón* de la versión de la clave que se desea activar.

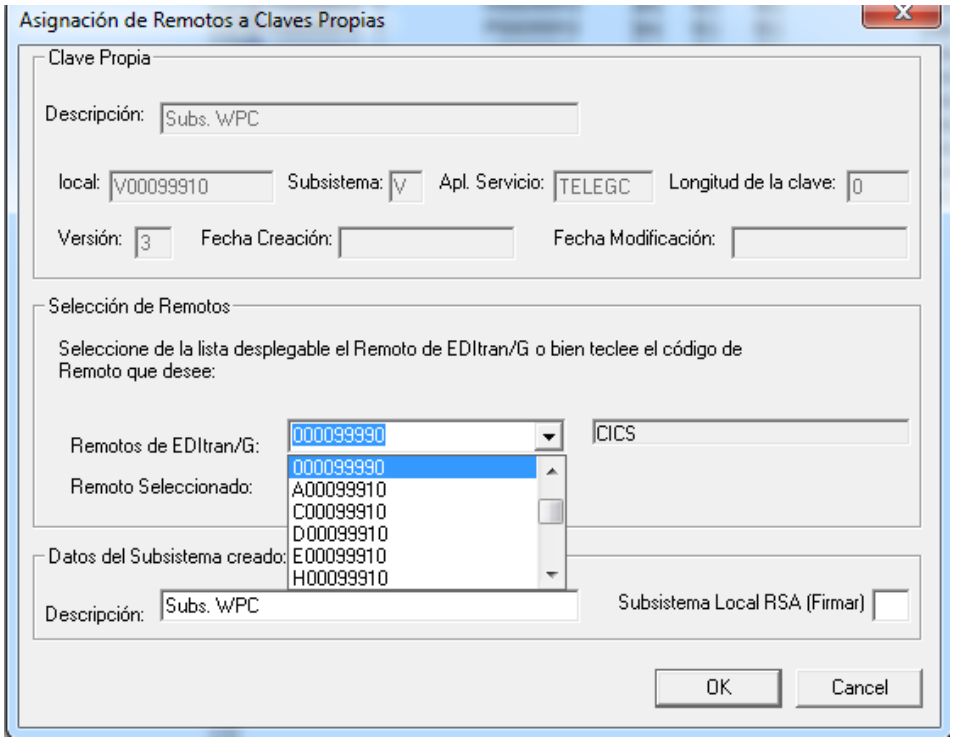
3.1.1.5.Asociación de Claves a Remotos

Una vez tengamos una Clave Propia, tendremos que crear el Subsistema Local RSA para ello hay que asignarle un Código Remoto.

Para asociar una Clave Propia a un remoto tendremos que seleccionar la clave propia desde la lista de Claves Propias que queremos asignar y con el botón de la derecha seleccionar *Asignar un Remoto*:



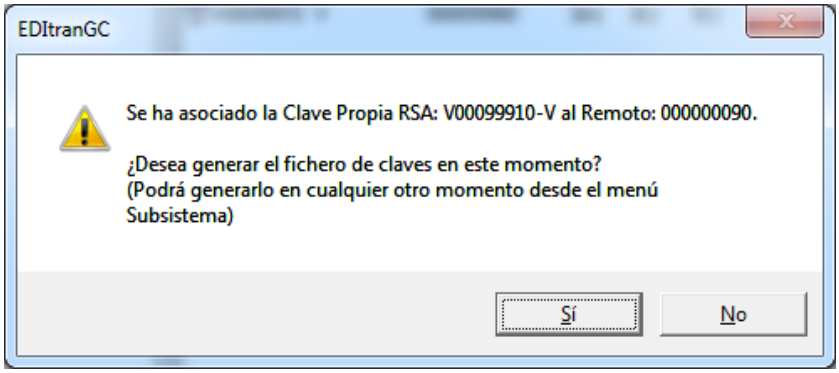
Aparece el dialogo de Asignación de Remotos a Claves Propias:



En la lista desplegable de Remotos de EDItran/G aparecen los códigos remotos que estén dados de alta en EDItran/G. Si no se tiene EDItran o si el código remoto no ha sido dado de alta todavía, se puede rellenar el campo '*Remoto Seleccionado*' con el código remoto que se le desea asignar a la Clave Propia.

Una vez asignado el remoto se generará automáticamente un nuevo Subsistema Local RSA.

A continuación se le da la opción al usuario de generar el fichero de intercambio que incluye la clave pública asignada al subsistema recientemente creado:


EDItranGC
Se ha asociado la Clave Propia RSA: V00099910-V al Remoto: 000000090.
¿Desea generar el fichero de claves en este momento?
(Podrá generarlo en cualquier otro momento desde el menú Subsistema)
Sí
No

Si pulsamos *Sí* generaremos el fichero de intercambio para enviarlo al remoto. No es imprescindible generar el fichero en éste momento, podremos generarlo en cualquier otro momento (consultar los apartados **3.1.2.1 Producción del fichero de intercambio** y **3.1.2.2 Envío del fichero al remoto**).

3.1.2. Subsistema Local RSA

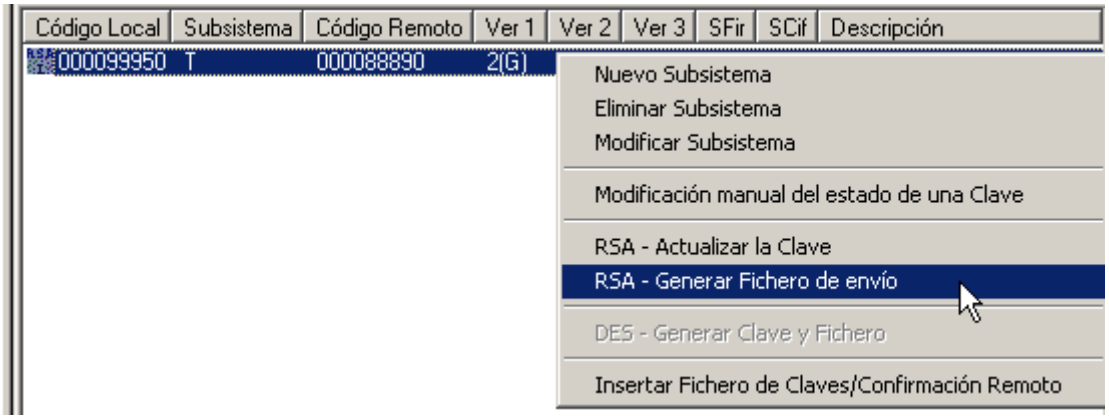
Como ya se ha explicado anteriormente, un subsistema local RSA se crear al asociar una Clave Propia RSA con un remoto.

En éste apartado se verá como enviar la clave generada al remoto y que otras iones se pueden realizar sobre el subsistema.

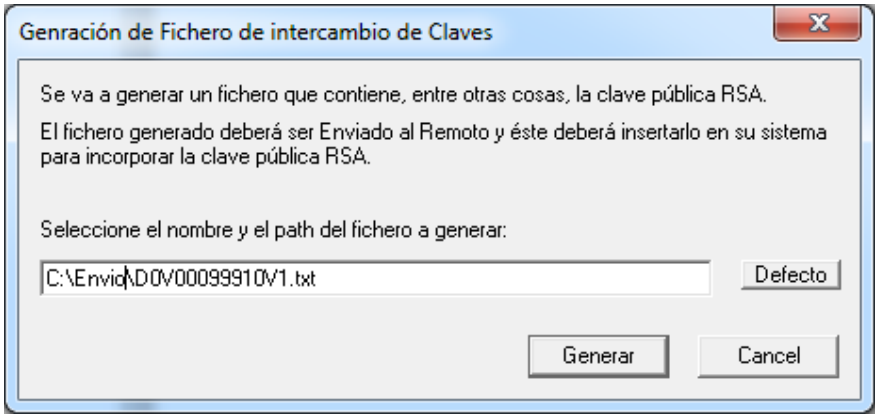
3.1.2.1.Producción del fichero de intercambio

El fichero de intercambio se puede generar de dos maneras:

- Al asignar un remoto a una Clave Propia, como se indica en **3.1.1.5 Asociación de Claves a Remotos**
- En cualquier momento utilizando la barra de herramientas, como se indica en el aparatado **2.3.4 Generar Fichero de Envío**.
- Seleccionando el subsistema local RSA de la lista y con el botón de la derecha elegir en el menú contextual que aparece:



Aparece el siguiente dialogo:


Genración de Fichero de intercambio de Claves
Se va a generar un fichero que contiene, entre otras cosas, la clave pública RSA.
El fichero generado deberá ser Enviado al Remoto y éste deberá insertarlo en su sistema para incorporar la clave pública RSA.
Seleccione el nombre y el path del fichero a generar:
C:\Envio\D0V00099910V1.txt
Defecto
Generar
Cancel

Hay que indicar el path del fichero donde se generará.

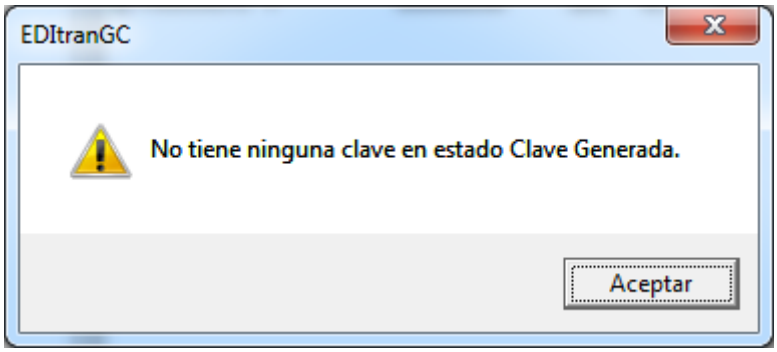
Si el subsistema contiene una *Aplicación de Servicio de EDItran/G* (Aplicación de EDItran/G que se utilizará para enviar el fichero de intercambio) el nombre del fichero que aparece por defecto será el que esté dado de alta en EDItran/G, así se asegura que el fichero generado se enviará correctamente.

Si el subsistema no contiene una *Aplicación de Servicio de EDItran/G* o bien esa aplicación no existe en EDItran, se muestra un nombre de fichero por defecto, que puede ser modificado, y que no podrá ser enviado automáticamente por EDItran.

Para poder generar un fichero de intercambio es indispensable que algunas de las tres claves almacenadas en el subsistema tenga el estado *"Clave Generada(G)"*. Esto ocurre cuando:

- Se acaba de crear el subsistema local RSA al asociar una Clave Propia a un Remoto (ver apartado **3.1.1.5 Asociación de Claves a Remotos**).
- Se Actualiza la clave de un subsistema local RSA con una versión mayor (ver apartado **3.1.2.3 Actualización de claves del subsistema**)

Si no se dan estas circunstancias y ninguna de las versiones de las claves se encuentra en estado *"Clave Generada(G)"*, no se podrá generar el fichero de envío. Aparece el siguiente dialogo indicándolo:



En circunstancias especiales es posible que se desee enviar el fichero de intercambio para una clave que no esté en estado *"Clave Generada(G)"*. Para conseguirlo habrá modificar manualmente el estado de la versión de la clave que se desea enviar (ver aparatado 3.3.3).

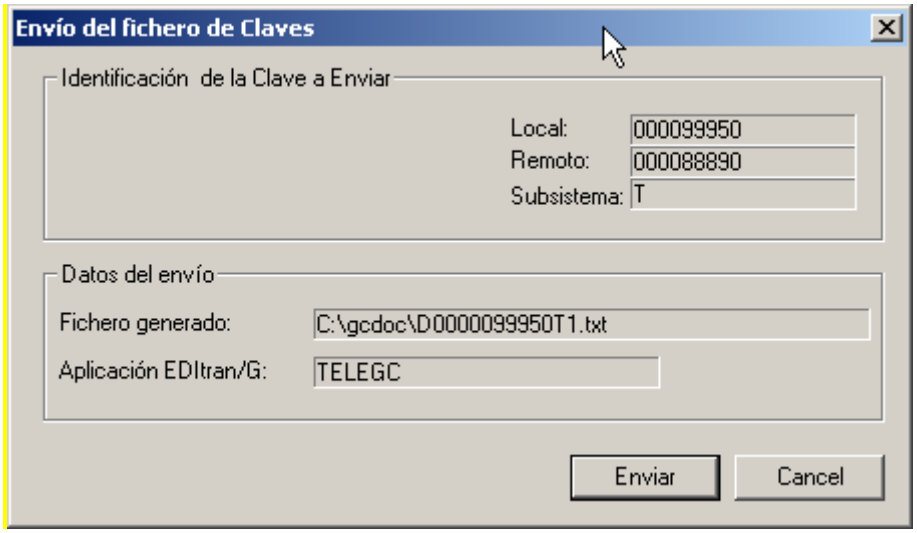
Una vez generado el fichero de intercambio y si el subsistema contiene una *Aplicación de Servicio de EDItran/G*, entonces se intentará enviar el fichero por EDItran.

3.1.2.2.Envío del fichero al remoto

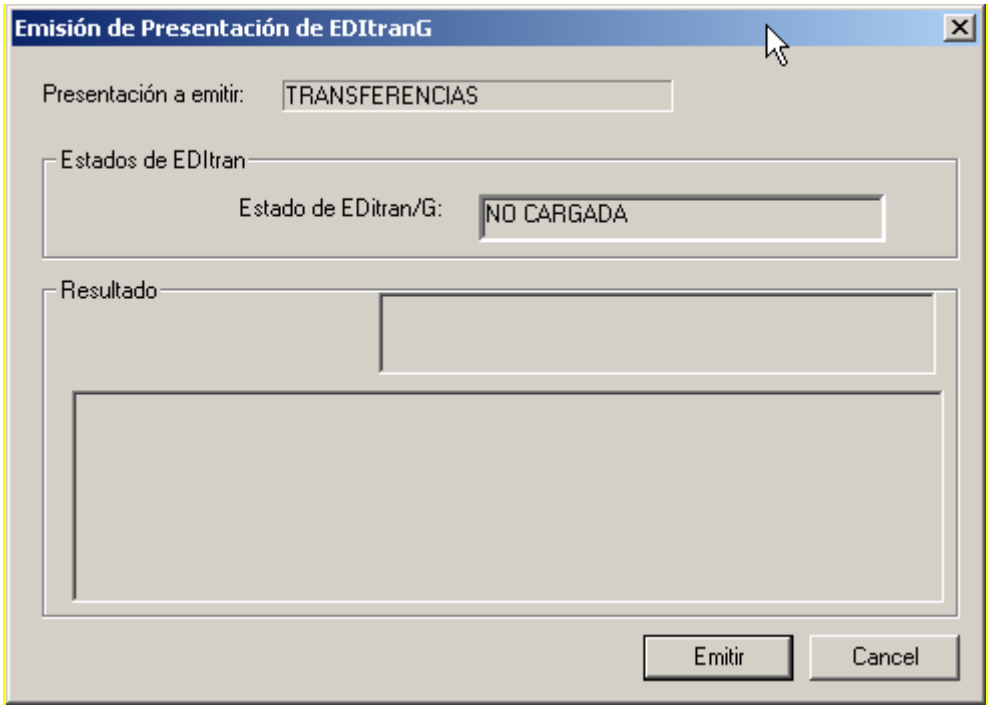
El fichero puede enviarse automáticamente por EDItran o bien enviarse por cualquier otro medio al remoto. Es aconsejable utilizar EDItran porque está perfectamente integrado en el intercambio de claves y permite automatizar el proceso.

❑ **Envío por EDItran**

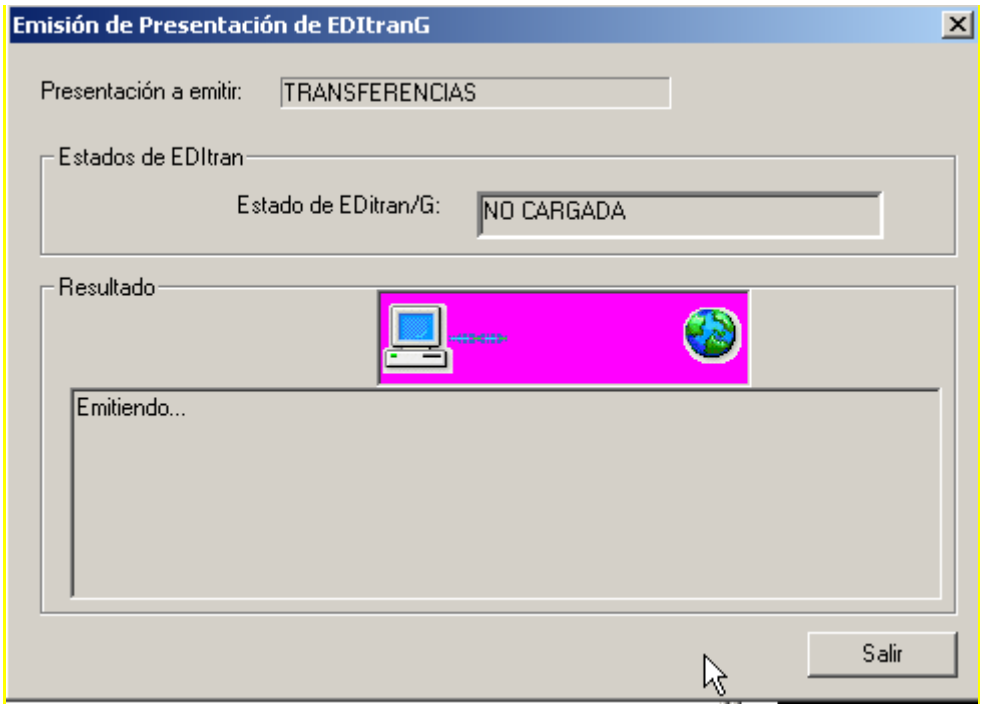
Como se explicó en el apartado anterior, cuando se genera un fichero de intercambio, y si el subsistema contiene una *Aplicación de Servicio de EDItran/G*, se da la posibilidad de enviarlo por EDItran:



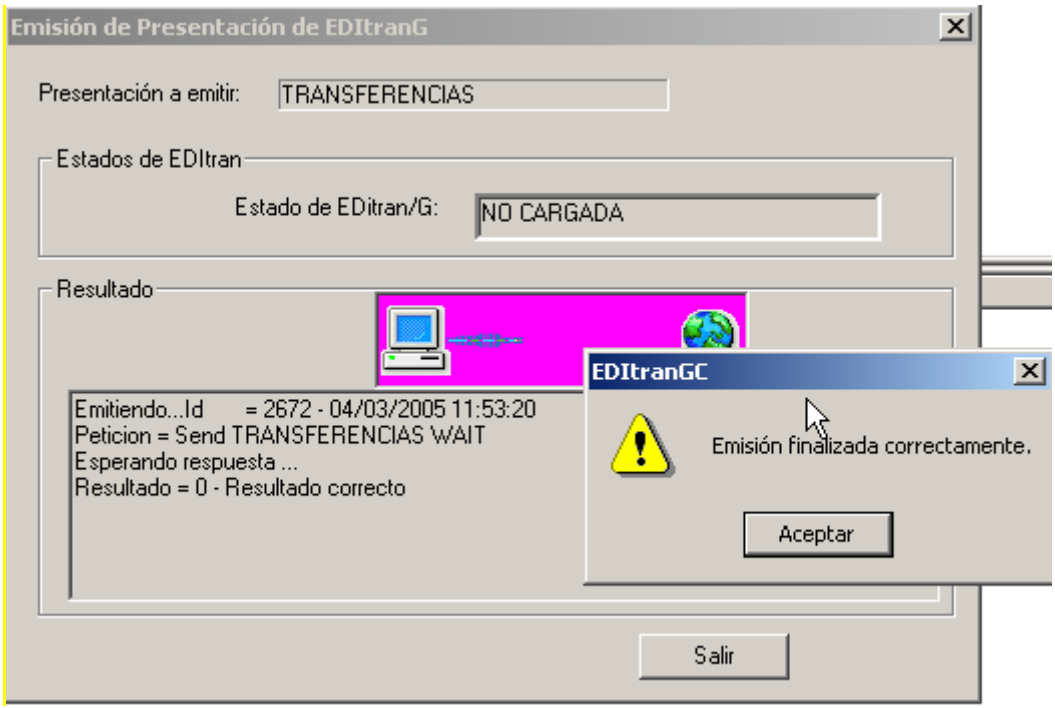
Aparece la información del código local, código remoto y el subsistema que se enviará. Al pulsar Enviar y aparece el dialogo:



Indicando la presentación por la que se emitirá el fichero de intercambio y el estado de EDItran/G en que se encuentra la Presentación. Pulsando 'Emitir' se pedirá una emisión a EDItran:

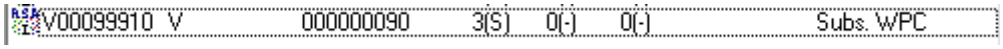


Al finalizar indicará si la emisión ha finalizado correctamente o si ha habido algún error:

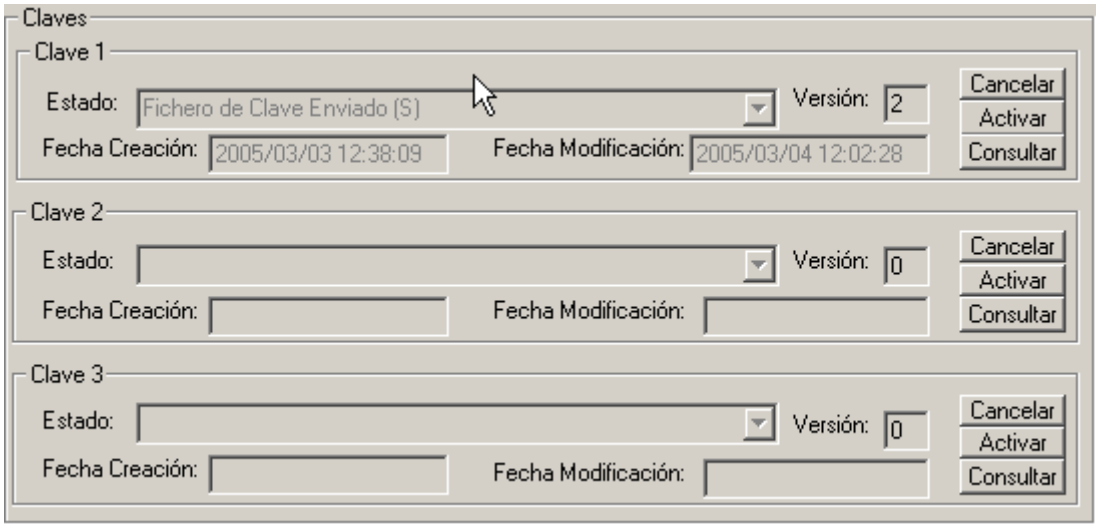


Si todo ha ido bien se cambiará el estado de la clave a *"Fichero de Clave Enviado (S)"*.

En la lista se verá que la versión tiene estado (S) :



Y en el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1 Modificación, Consulta y Eliminación de un subsistema Local RSA**) veremos el estado y la fecha de creación de la clave y de modificación del estado:



Si la transmisión no finaliza correctamente, el estado de la versión de la clave se cambiará a *"Error al Enviar Fichero de Clave (E)"*.

3.1.2.3.Actualización de claves del subsistema

Si se ha creado una nueva versión de una Clave Propia (consultar el apartado **0**) habrá que actualizar los subsistemas que están asociados a esa Clave Propia.

Para eso se pincha sobre el botón de *Actualización de Clave* o se selecciona *RSA-Actualizar la clave* desde el menú contextual que aparece al pulsar con el botón de la derecha sobre la lista de subsistemas locales RSA. Para más información consultar los apartados **2.3.5** y **3.1.1.4**.

La versión de la clave que esté activa dentro de la Clave Local, se copiará al subsistema. Después habrá que generar el fichero de intercambio y enviarlo al remoto como se explica en los apartados **3.1.2.1** y **3.1.2.2**.

3.1.2.4.Versión de la Clave en vuelo

Sólo puede haber una versión de la clave en vuelo dentro de un mismo subsistema. Por tanto mientras exista una clave en vuelo no se permitirá la creación de más versiones de claves.

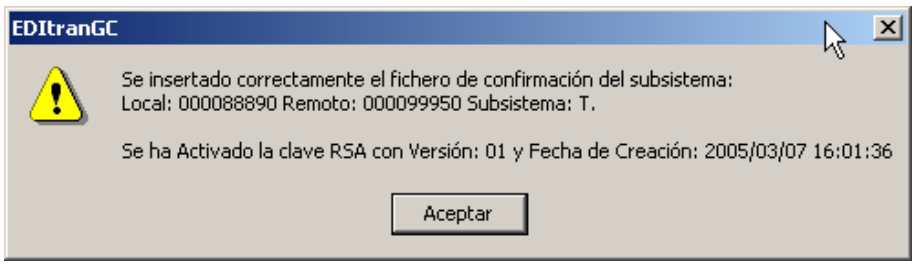
Una clave se considera *en vuelo* cuando se encuentra en el proceso de activación es decir cuando ya existe la clave pero aún no se ha enviado al remoto y no se ha recibido el fichero de confirmación de éste. Una vez confirmada, la clave pasa a estado "*Activa*" y dejar de estar en vuelo, permitiendo que se puedan generar nuevas versiones.

Una versión de la clave que esté *en vuelo* puede dejar de estarlo *Activándola* o *Cancelándola* manualmente (ver sección **3.3.4**).

3.1.2.5.Inserción de un fichero de confirmación

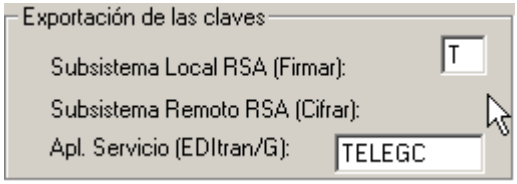
Una vez que el remoto haya insertado nuestra clave pública (ver apartado **3.2**) nos enviará un fichero de confirmación. Este fichero nos indica que el remoto incorporó la clave correctamente y así podemos nosotros activar la clave para que pueda ser utilizada con ese remoto.

Si estamos utilizando EDItran y tenemos el automatismo posterior a recepción de EDItran/GC, entonces al recibir la confirmación, automáticamente se activará la clave. Si no es así, entonces tendremos que insertar el fichero de confirmación pulsando sobre el botón "Inserción de fichero de Claves/Confirmación" de la barra de herramientas (ver apartado **2.3.7**). Aparecerá un dialogo indicando los datos de la confirmación:


EDItranGC
Se insertado correctamente el fichero de confirmación del subsistema:
Local: 000088890 Remoto: 000099950 Subsistema: T.
Se ha Activado la clave RSA con Versión: 01 y Fecha de Creación: 2005/03/07 16:01:36
Aceptar

Ahora ya se dispone de una clave *"Activa"* para ese subsistema con ese remoto. Lo que significa que los intercambios posteriores ya pueden y deben ir firmados, ya que al haber intercambiado la clave pública, debe utilizarse ésta para firmar futuros envíos de claves.

En éste caso debería modificarse el subsistema (ver apartado **3.3.1**) para que vaya firmado con el subsistema 'T':



3.2. Generación de un Subsistema Remoto RSA y envío de la confirmación

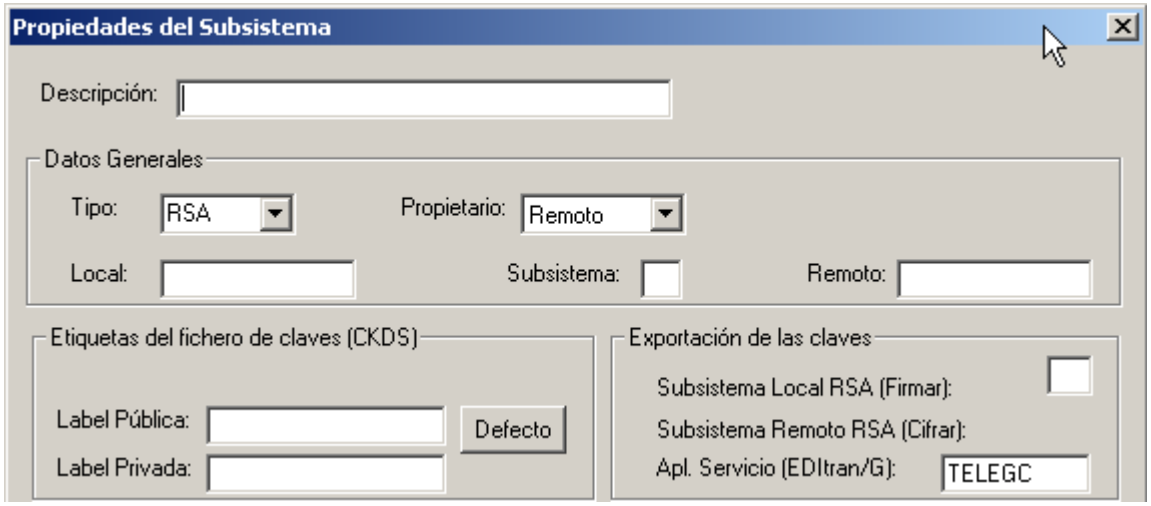
Se puede generar un subsistema remoto de tres formas, dos manuales y una automática:

- Automáticamente utilizando el programa de usuario de EDItran/G posterior a recepción (mirar sección XXXXXXXXXXXXXXXXXXX)
- Manualmente a través de la interfaz gráfica pinchando sobre el botón de la barra de herramientas *"Nuevo Subsistema"*.
- Manualmente a través de la interfaz gráfica pinchando sobre el botón de la barra de herramientas *"Inserción de fichero remoto"*.

En este apartado veremos las dos maneras manuales de añadir un subsistema remoto.

3.2.1. Generación de un Subsistema Remoto RSA

Para generar un subsistema Remoto RSA, pinchar sobre el botón "Crear un Subsistema" de la barra de herramientas (ver apartado **2.3.1**). Aparecerá el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**) , seleccionar Tipo a *"RSA"* y Propietario a *"Remoto":*



Se rellenan los datos de código local, código remoto y subsistema, opcionalmente se rellena la Descripción y se pulsa defecto para obtener las labeles por defecto, de ésta manera se asegura que no haya ninguna label repetida.

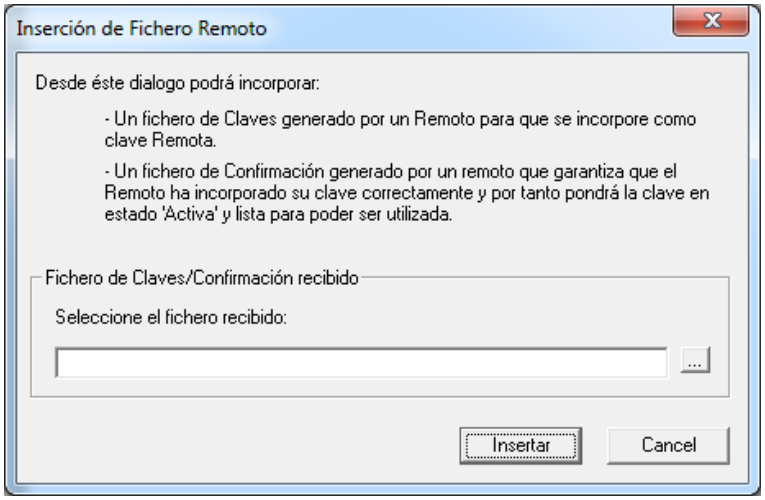
Si el fichero de intercambio viene firmado habrá que poner el subsistema local RSA que se ha utilizado para firmar y si viene cifrado habrá que poner el subsistema remoto rsa.

La aplicación de servicio de EDItran/G se utiliza si se quiere enviar las confirmaciones por EDItran. Se recomienda utilizar la Aplicación de EDItran/G TELEG.

Pulsando sobre el botón *"OK"*, se generará un nuevo subsistema remoto RSA. Sin embargo aún no se tiene la clave pública necesaria. Está se tendrá que añadir manualmente como se explica en el apartado siguiente o automáticamente mediante los automatismos de EDItran/G.

3.2.2. Incorporación de un fichero de intercambio remoto

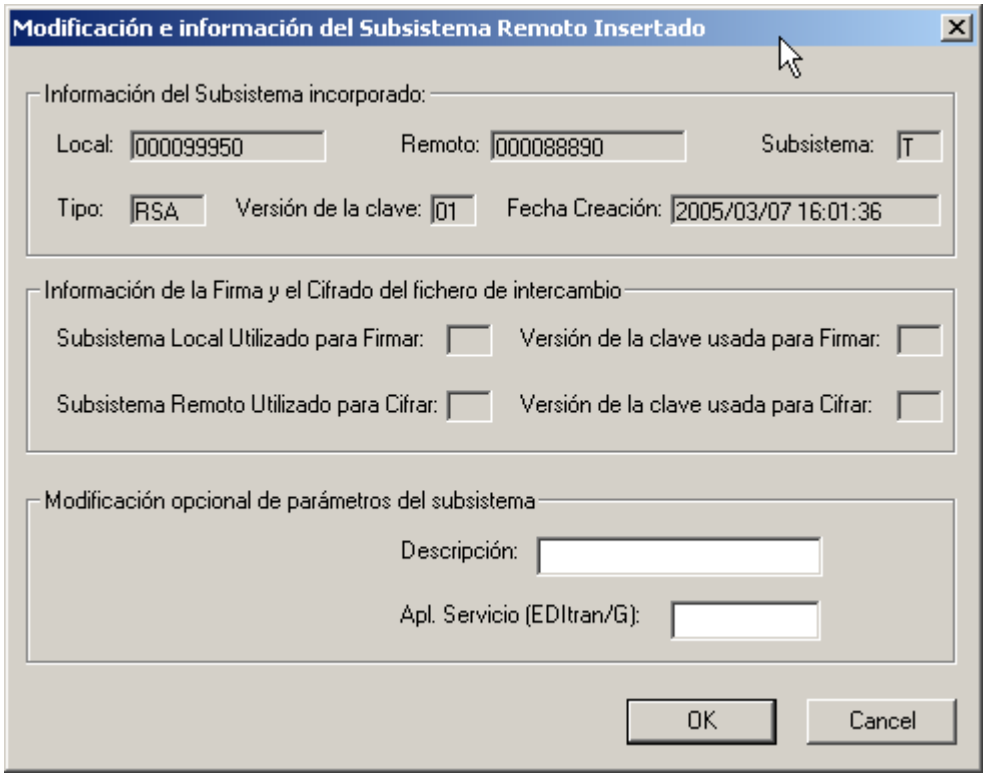
Al pinchar sobre el botón *"Inserción de Fichero Remoto"* aparecerá el dialogo:


Inserción de Fichero Remoto
Desde éste dialogo podrá incorporar:
- Un fichero de Claves generado por un Remoto para que se incorpore como clave Remota.
- Un fichero de Confirmación generado por un remoto que garantiza que el Remoto ha incorporado su clave correctamente y por tanto pondrá la clave en estado 'Activa' y lista para poder ser utilizada.
Fichero de Claves/Confirmación recibido
Seleccione el fichero recibido:
...
Insertar
Cancel

Se debe seleccionar el fichero de intercambio recibido por el remoto y pulsar Insertar.

EDItran/GC primero comprueba la firma del fichero de intercambio, luego, si el subsistema que viene en el fichero no ha sido de alta previamente (como se indica en el apartado 3.2.1) se genera automáticamente con los datos del fichero y por último se incorpora la clave pública del remoto en el fichero de claves de EDItran (ckds.rsa).

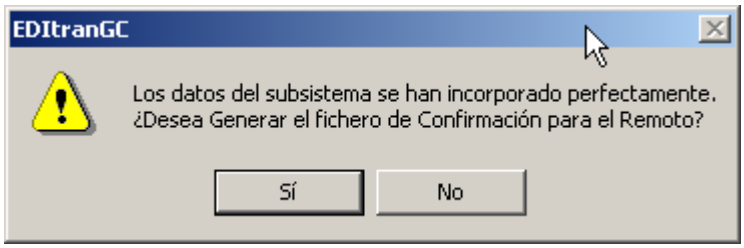
Una vez finalizado el proceso, aparece un dialogo mostrando la clave del subsistema que ha incorporado:


Modificación e información del Subsistema Remoto Insertado
Información del Subsistema incorporado:
Local: 000099950
Remoto: 000088890
Subsistema: T
Tipo: RSA
Versión de la clave: 01
Fecha Creación: 2005/03/07 16:01:36
Información de la Firma y el Cifrado del fichero de intercambio
Subsistema Local Utilizado para Firmar:
Versión de la clave usada para Firmar:
Subsistema Remoto Utilizado para Cifrar:
Versión de la clave usada para Cifrar:
Modificación opcional de parámetros del subsistema
Descripción:
Apl. Servicio (EDItran/G):
OK
Cancel

La primera vez que se intercambia un subsistema con un remoto, el fichero no viene firmado porque no se tiene ninguna clave con la que verificar su firma. En sucesivos intercambios de versiones de claves, el fichero de intercambio deberá venir firmado.

Además aparecen dos campos para introducir, de forma opcional, una descripción del subsistema generado o la Aplicación de servicio por la que viajará el fichero de confirmación.

Al pulsar sobre el botón *"OK"* se nos da la opción de generar el fichero de confirmación:

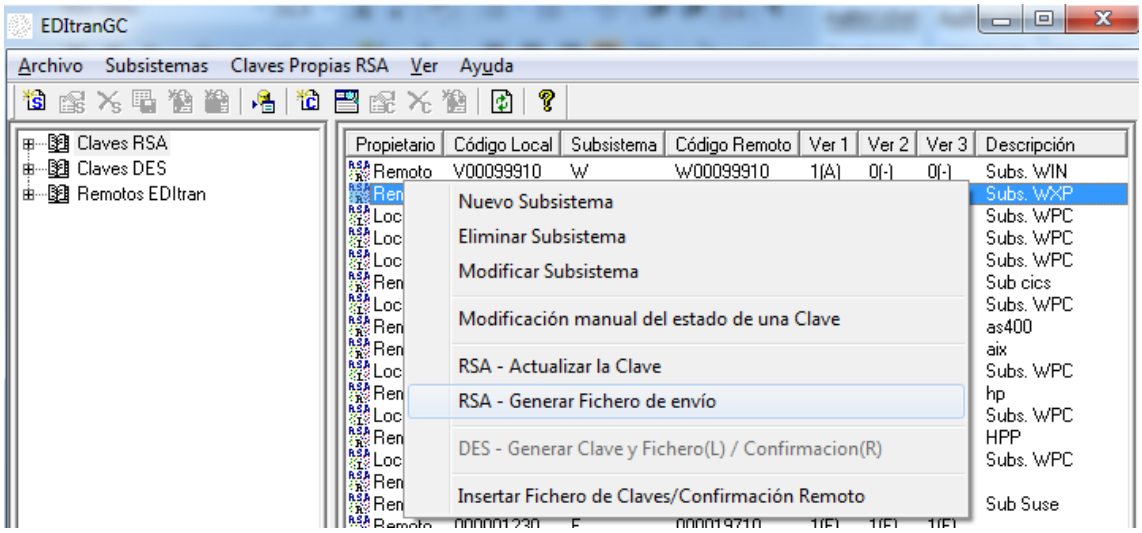

EDItranGC
Los datos del subsistema se han incorporado perfectamente.
¿Desea Generar el fichero de Confirmación para el Remoto?
Sí
No

Si pulsamos "Si" se genera el fichero de confirmación. No es obligatorio generar el fichero de confirmación en éste momento ya que lo podremos generar en otro momento posterior, sin embargo es recomendable generar el fichero en éste momento.

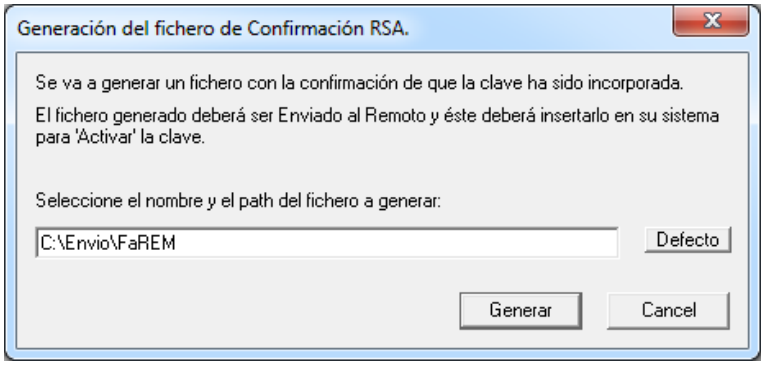
3.2.3. Generación y envío de la confirmación

Al incorporar una clave pública RSA remota, se debe generar un fichero de confirmación que se enviará al remoto para que éste pueda comprobar que el proceso de incorporación se ha efectuado correctamente y así pasar la clave a estado *"Activa"* para que pueda ser utilizada por EDItran.

Como se ha indicado antes la confirmación se puede generar en el momento de inserción de la clave pública RSA del remoto. Pero también se puede generar (de no haberse generado antes) en cualquier momento. Para eso se selecciona el subsistema remoto RSA que queremos confirmar, pinchando con el botón derecho y escogiendo *"RSA - Generar Fichero de envío":*



Tanto de manera automática (al insertar la clave) como de manera manual (en cualquier momento posterior como se acaba de indicar), aparece un dialogo donde se puede indicar el path del fichero de confirmación que se generará:


Generación del fichero de Confirmación RSA.
Se va a generar un fichero con la confirmación de que la clave ha sido incorporada.
El fichero generado deberá ser Enviado al Remoto y éste deberá insertarlo en su sistema para 'Activar' la clave.
Seleccione el nombre y el path del fichero a generar:
C:\Envio\FaREM
Defecto
Generar
Cancel

Si el subsistema tiene una Aplicación de Servicio de EDItran/G (típicamente será 'TELEG'), se intentará enviar el fichero por EDItran como se indica en el apartado □). Una vez generado el fichero y enviado por EDItran, se activará ésta versión de la clave, asegurándonos el intercambio seguro de ficheros con la versión de la última clave generada.

3.3. Otras operaciones comunes sobre los subsistemas

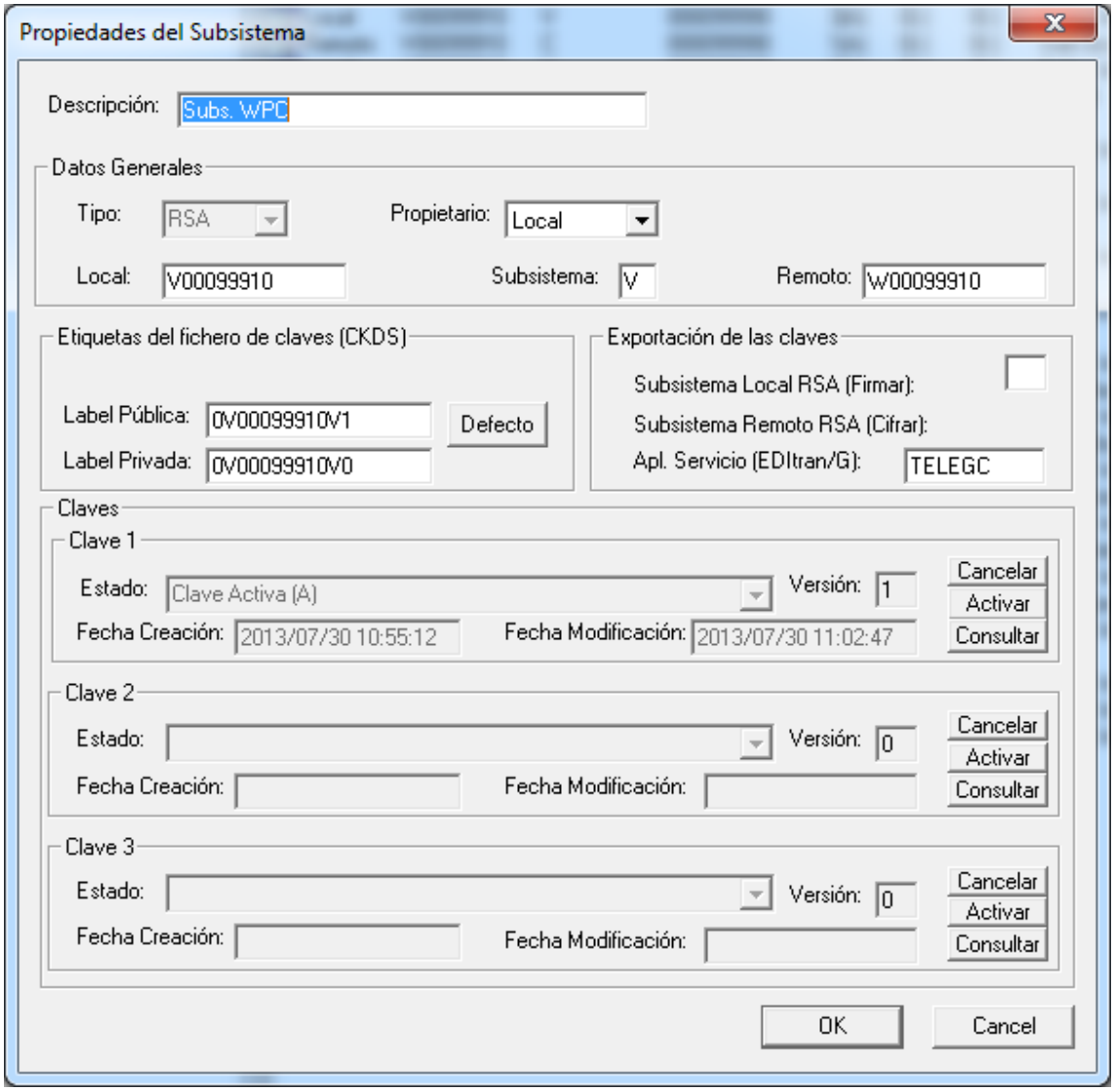
A continuación se detallarán funcionalidades comunes de los subsistemas Locales y Remotos de RSA.

3.3.1. Modificación, Consulta y Eliminación de un subsistema Local RSA

Para ver todas los subsistemas locales de RSA podemos selecciona en el árbol la rama adecuada (ver apartado **0**) o bien pulsar sobre el botón de *Mostrar Claves Propias RSA* de la barra de Herramientas (ver apartado **2.3.9**).

Para Eliminar un subsistema, seleccionarlo de la lista y pulsar <Del> o <Supr>.

Para Modificar o Consultar un subsistema, hacer doble clic sobre la línea de la lista. Aparece el dialogo de *Propiedades del Subsistema*:

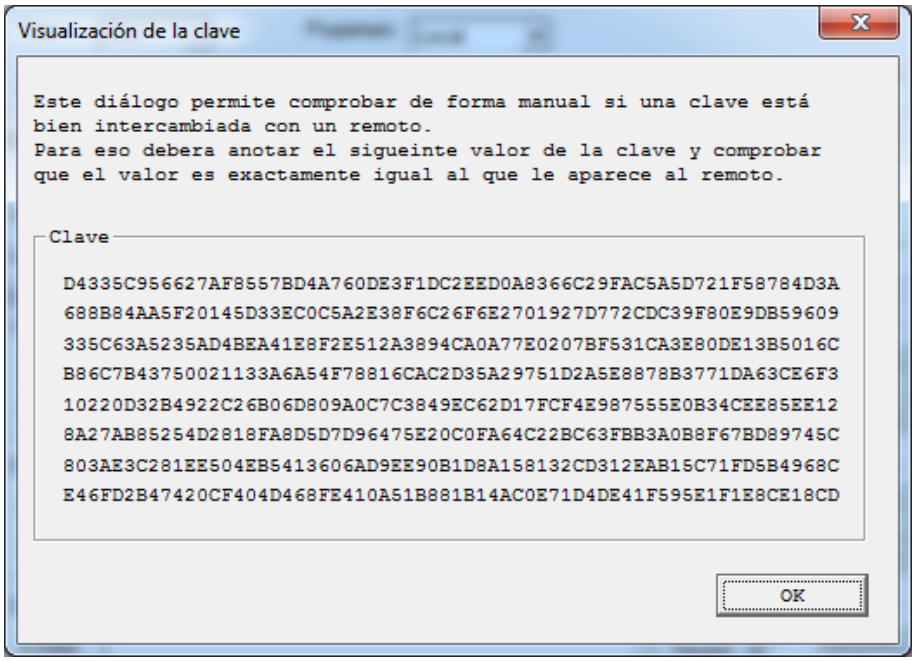


Desde aquí se pueden realizar las siguientes operaciones:

- Cambio de propiedades y ***modificación del subsistema***, pulsando el botón *"OK"*
- ***Consultar una versión de la clave***, pulsando sobre el botón *"Consultar"* de la versión de la clave (ver apartado **3.3.2**)
- ***Activar una versión de la clav***e, pulsando sobre el botón *"Activar"* de la versión de la clave que se desee activar (ver apartado **3.3.4**).
- ***Cancelar una versión de la clave***, pulsando sobre el botón *"Cancelar"* de la versión de la clave que se desee cancelar (ver apartado **3.3.4**).

3.3.2. Consulta de claves RSA

Al pulsar sobre el botón *Consultar* de una versión del dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**) se verá su clave pública:


Visualización de la clave
Este diálogo permite comprobar de forma manual si una clave está bien intercambiada con un remoto.
Para eso debera anotar el sigueinte valor de la clave y comprobar que el valor es exactamente igual al que le aparece al remoto.
Clave
D4335C956627AF8557BD4A760DE3F1DC2EED0A8366C29FAC5A5D721F58784D3A
688B84AA5F20145D33EC0C5A2E38F6C26F6E2701927D772CDC39F80E9DB59609
335C63A5235AD4BEA41E8F2E512A3894CA0A77E0207BF531CA3E80DE13B5016C
B86C7B43750021133A6A54F78816CAC2D35A29751D2A5E8878B3771DA63CE6F3
10220D32B4922C26B06D809A0C7C3849EC62D17FCF4E987555E0B34CEE85EE12
8A27AB85254D2818FA8D5D7D96475E20C0FA64C22BC63FBB3A0B8F67BD89745C
803AE3C281EE504EB5413606AD9EE90B1D8A158132CD312EAB15C71FD5B4968C
E46FD2B47420CF404D468FE410A51B881B14AC0E71D4DE41F595E1F1E8CE18CD
OK

Esta funcionalidad es útil para comparar la clave local propia, que hemos generado y permanece en nuestro sistema, con la Clave Remota RSA que el remoto habrá insertado en su sistema, incorporando el fichero de intercambio que habremos generado.

3.3.3. Modificación manual del estado de una clave RSA

La modificación manual del estado de una clave puede ser una operación peligrosa ya que puede dejar inestable el subsistema al que se realice el cambio.

Sin embargo, en algunos casos, puede ser útil modificar manualmente el estado en que se encuentra alguna clave. Por ejemplo:

- Se ha enviado el fichero de intercambio con una clave RSA pero el remoto no lo ha podido incorporar y se ha eliminado fichero. En esta circunstancia hay que crear de nuevo el fichero de intercambio modificando el estado de la versión de la clave a *"Clave Generada (G)"*.
- Ha habido un error al enviar el fichero por EDItran y el estado se ha quedado en *"Error al Enviar Fichero de Clave (E)"* o *"Error al Enviar Fichero de Confirmación (E)"* sin embargo se ha solucionado el problema el problema y el fichero se ha enviado manualmente por EDItran. Entonces habrá que modificar el estado a *"Fichero de Claves Enviado (E)"* o *"Fichero de Confirmación Enviado(S)"* respectivamente.

Es recomendable no modificar manualmente el estado de una clave si no se conocen perfectamente el efecto que la modificación puede producir.

3.3.4. Activación y Cancelación de una clave RSA

Mediante el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**) se puede activar o cancelar una versión de una clave del subsistema.

Sólo puede haber una versión de una clave en estado *"Activa (A)"* en un subsistema. Cuando se activa una clave, ya sea automáticamente o manualmente, si otra clave estaba antes *"Activa (A)"*, entonces pasará a estado *"Operativa (O)"*. Para activar una versión de la clave, se debe pulsar el botón *"Activar"* de el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**).

También se puede cancelar una versión de una clave. Cancelando la clave se asegura que la clave no pueda ser utilizada. Para cancelar una versión de la clave, se debe pulsar el botón *"Cancelar"* de el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**).

4. Intercambio de claves DES

DES (Data Encryption Standard) es un esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores. Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de USA.

La criptografía DES es muy utilizada gracias a la rapidez de los cálculos de cifrado y descifrado, sin embargo, la criptografía simétrica tiene el inconveniente de que los dos extremos deben tener la misma clave y por tanto deben intercambiarla de una manera segura.

Para el intercambio seguro de las claves simétricas, se desarrollaron las claves asimétricas, como RSA, que como ya se ha visto, la clave pública puede ser intercambiada previamente y ser utilizada posteriormente para cifrar un intercambio de una clave DES.

EDItran/GC soluciona esta problemática y simplifica el proceso de intercambio, generando además nuevas versiones de claves y administrando toda la información de manera clara y sencilla.

4.1. Subsistema Local DES

El fichero de intercambio de claves DES se genera de forma que se garantiza:

- ***Confidencialidad***: El emisor cifra el texto con la clave pública del receptor y el receptor lo descifra con su clave privada. Así cualquier persona puede enviar un mensaje cifrado, pero solo el receptor, que tiene la clave privada, puede descifrar el contenido.
- ***Autenticación***: Se cifra el mensaje o un resumen de éste mediante la clave privada y cualquier persona puede comprobar su procedencia utilizando la clave pública del emisor. El mensaje es auténtico porque solo el emisor verdadero puede cifrar con su clave privada.
- ***Integridad***: Asegura que el mensaje se transfiere intacto gracias a que la firma depende no sólo de la identidad del remitente sino también del contenido del mismo.
- ***No Repudio***: Impide que el emisor pueda rechazar o repudiar un mensaje, es decir, negar su autoría sobre la información que envía y sus posibles consecuencias.

Por tanto, se necesita una clave privada RSA con la que firmar los datos y una clave pública RSA con la que cifrarlos.

En el lenguaje de EDItranGC, para poder intercambiar una clave DES con un remoto es necesario tener previamente un subsistema RSA Local asociado al remoto con una clave en estado activa (clave privada usada para firmar) y un subsistema RSA Remoto con una clave activa (clave publica usada para cifrar.

4.1.1. Creación de un subsistema Local DES

4.1.1.1.Requisitos previos

Como se ha explicado, antes de generar un subsistema Local DES, hay que generarse previamente un subsistema RSA Local, que se utilizará para firmar los datos del fichero de intercambio y hay que recibir un subsistema RSA Remoto que se utilizará para cifrar los datos del mismo fichero.

Además, debe existir una clave activa en cada uno de los dos subsistemas RSA necesarios.

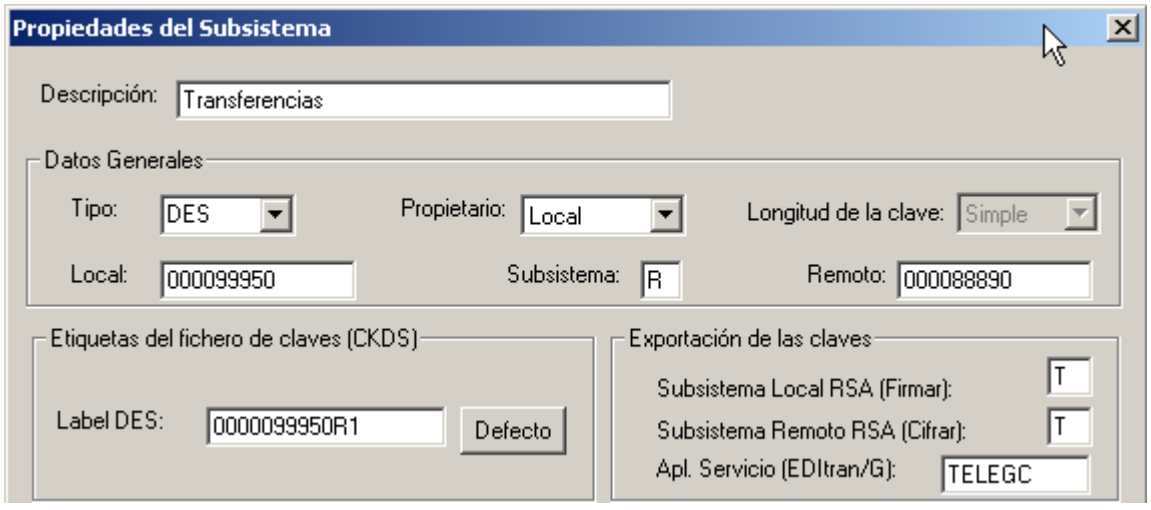
Cuando se cumplen estos requisitos, ya es posible generar un subsistema Local DES.

4.1.1.2.Creación del subsistema

Para generar un subsistema Local DES, pinchar sobre el botón "Crear un Subsistema" de la barra de herramientas (ver apartado **2.3.1**). Aparecerá el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**) , seleccionar Tipo a *"DES"* y Propietario a *"Local".*

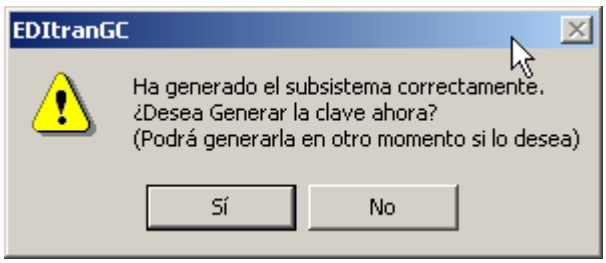
Se deben rellenar los campos *Local*, *Subsistema* y *Remoto*, una vez rellenos, pulsando sobre el botón '*Defecto'* se rellenará el campo *Label DES*.

Por último, faltan rellenar los campos de exportación de las claves. En el campo *Subsistema Local RSA (Firmar)* se pondrá el subsistema Local RSA que hayamos intercambiado con el remoto y que será usado para firmar el fichero de intercambio. En el campo *Subsistema Remoto RSA (Cifrar)* se pondrá el subsistema Remoto RSA que hayamos incorporado del remoto y que será usado para cifrar el fichero de intercambio:

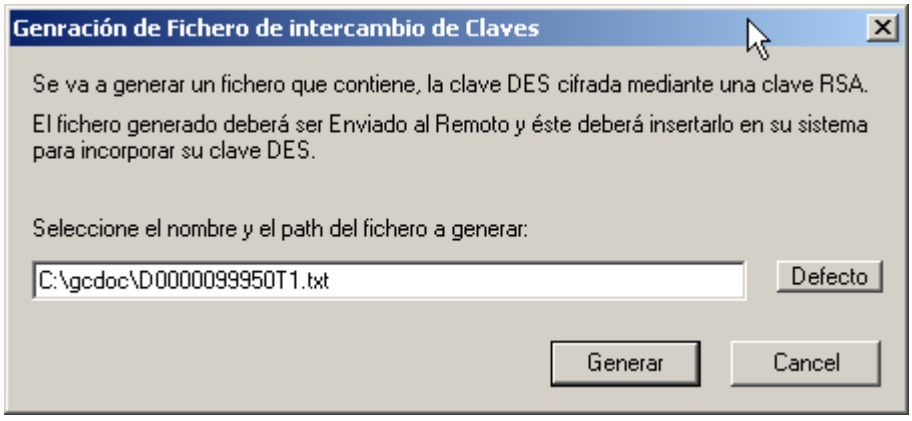


La aplicación de servicio de EDItran/G se utiliza si se quiere enviar el fichero de intercambio por EDItran. Se recomienda utilizar la Aplicación de EDItran/G TELEG.

Pulsando sobre el botón *"OK"*, se generará un nuevo subsistema local DES y se preguntará si se desea generar en ese momento la clave DES:

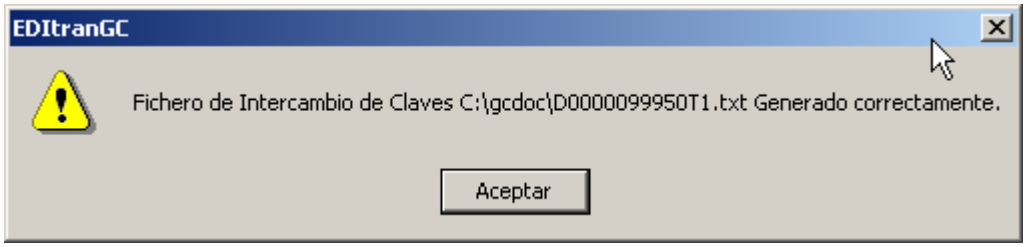


En el caso de claves DES, se debe generar el fichero de intercambio en el mismo momento que se genera la clave. Por motivos de seguridad, al ser una clave simétrica DES, nunca más se podrá volver a generar el fichero de intercambio. Por tanto si pulsamos afirmativamente a pregunta del anterior dialogo (*¿Desea generar la clave ahora?*) aparecerá el dialogo donde indicamos el path donde se dejará el fichero de intercambio que se deberá enviar al remoto:


Genración de Fichero de intercambio de Claves
Se va a generar un fichero que contiene, la clave DES cifrada mediante una clave RSA.
El fichero generado deberá ser Enviado al Remoto y éste deberá insertarlo en su sistema para incorporar su clave DES.
Seleccione el nombre y el path del fichero a generar:
C:\gcdoc\D0000099950T1.txt
Defecto
Generar
Cancel

Al pinchar sobre "Generar" se produce el siguiente proceso:

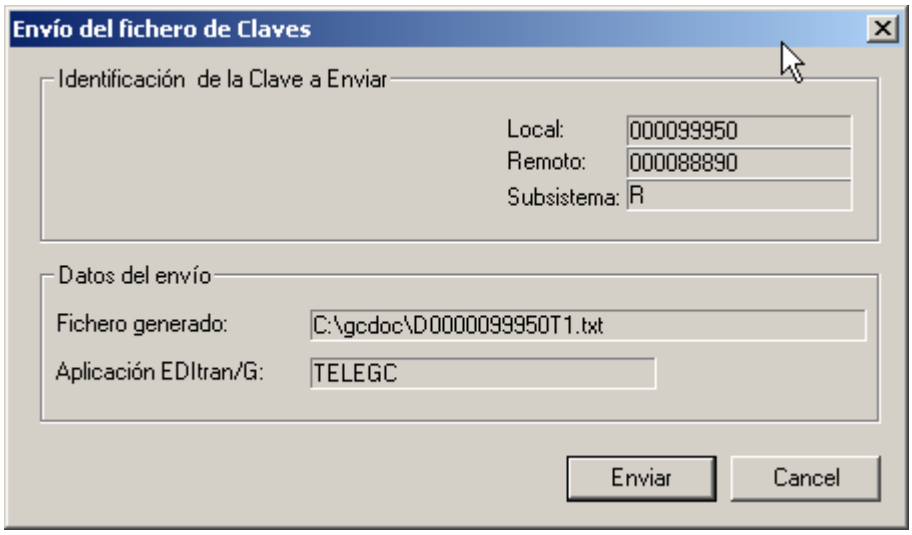
1. Generación de clave DES
2. Cifrado de la clave DES con la clave pública RSA del remoto
3. Generación de la firma con la clave privada RSA local
4. Generación del fichero de intercambio con la clave cifrada y la firma



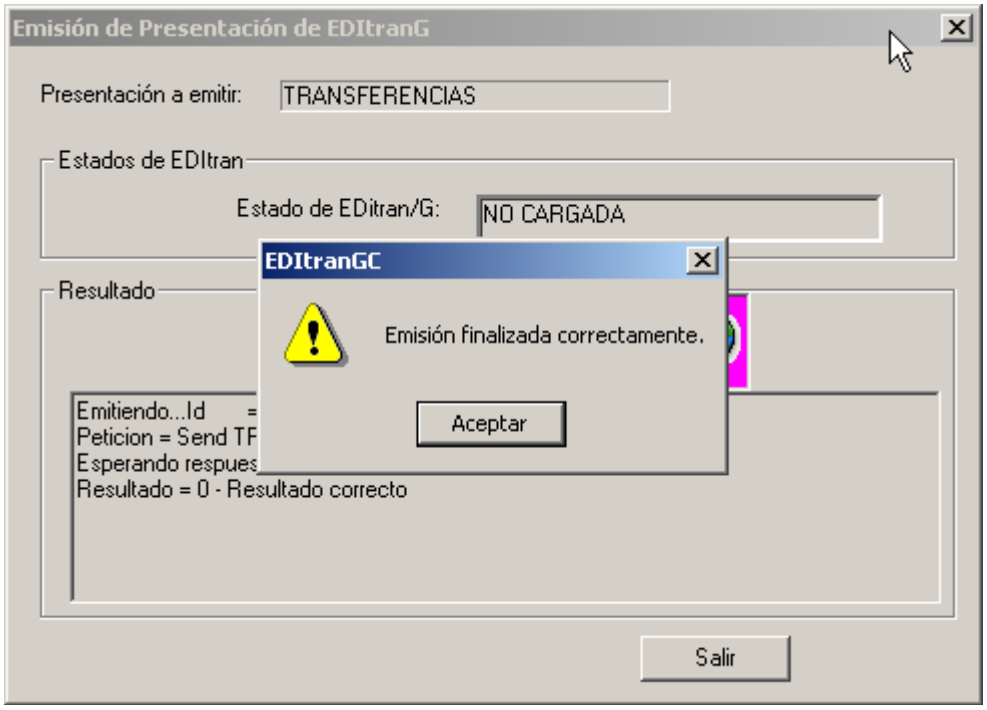
Si el subsistema está asociado a una Presentación de EDItran entonces, automáticamente se procederá al envío del fichero al remoto.

4.1.1.3.Envío del fichero de intercambio al remoto utilizando EDItran

El fichero de intercambio generado se puede enviar automáticamente por EDItran sin salirse del entrono de Editran/GC:

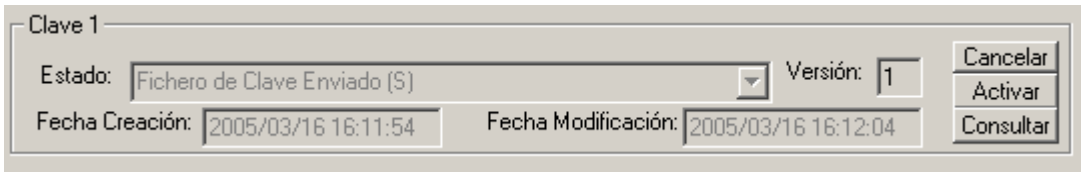


En el dialogo anterior se ven los datos de identificación de la clave (Local, Remoto y Subsistema) y los datos de envío (Fichero generado y la Aplicación de EDItran/G por la que se enviará). Pulsando '*Enviar*' se genera una petición de envío y veremos el resultado del mismo:



En ese momento la clave se queda en estado *"Fichero de Clave Enviado* (S)*"* a la espera de la confirmación del remoto:

Haciendo doble clic sobre la línea veremos el estado de la clave:



Cuando se reciba la confirmación la clave pasará a estado "Activa" y a partir de entonces podrá ser utilizada con total seguridad.

4.1.2. Generación de nuevas versiones de claves DES

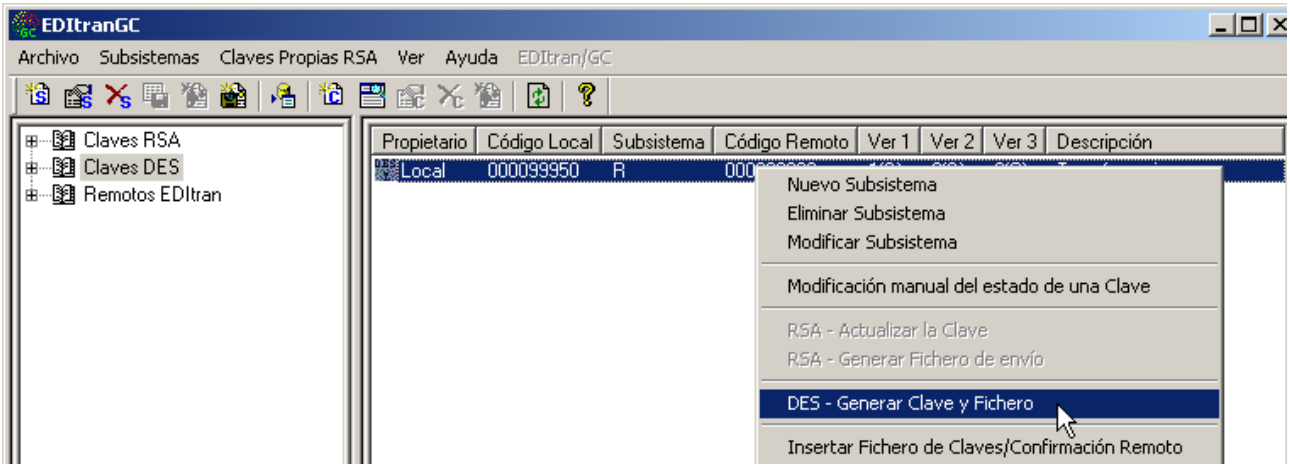
Para generar una nueva versión de una clave, es imprescindible que no exista ninguna versión de la clave *en vuelo* (ver sección **3.1.2.4**).

En el caso RSA, la nueva versión se genera sobre la *Clave Propia* y luego se actualiza en el subsistema que se desee. Sin embargo en DES, la clave se genera directamente en el propio subsistema. Esto es así porque en RSA una misma pareja de claves (formando una *Clave Propia*) puede estar asociada a n remotos (formando n subsistemas RSA) ya que la clave es asimétrica y nunca se intercambia la parte privada.

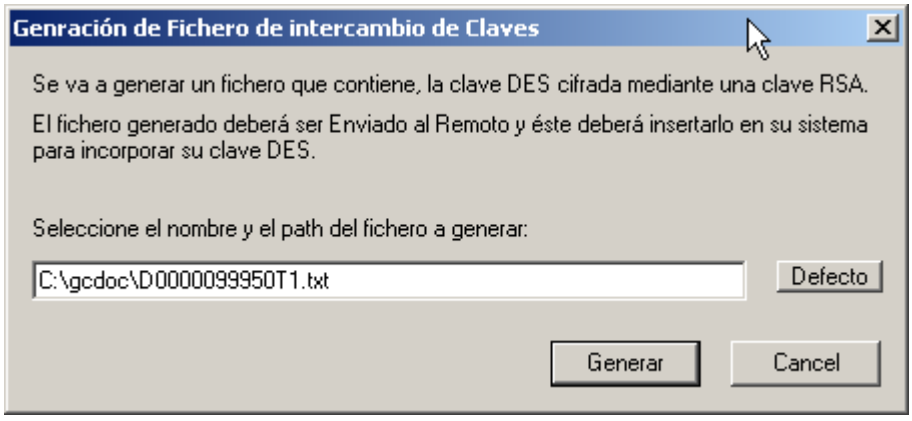
Por tanto, con RSA se puede compartir una clave y con DES no se puede, una clave DES está asociada a un único subsistema.

Existen tres maneras de generar una nueva versión de una Clave DES:

1. Pulsando sobre el botón Generar Nueva Clave DES del dialogo de Propiedades del Subsistema de una clave DES.
2. Seleccionando el menú: Subsistemas/DES - generar Clave y Fichero después de seleccionar el subsistema en la lista.
3. Pulsando el botón de la derecha sobre el subsistema DES que deseamos generar una nueva versión y /DES - generar Clave y Fichero.:

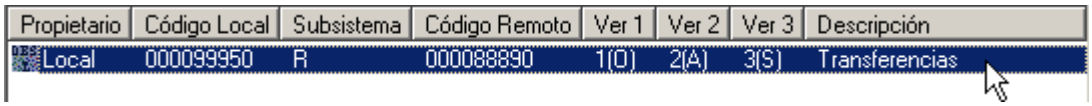

EDItranGC
Archivo Subsistemas Claves Propias RSA Ver Ayuda EDItran/GC
Claves RSA
Claves DES
Remotos EDItran
Propietario Código Local Subsistema Código Remoto Ver 1 Ver 2 Ver 3 Descripción
Local 000099950 R
Nuevo Subsistema
Eliminar Subsistema
Modificar Subsistema
Modificación manual del estado de una Clave
RSA - Actualizar la Clave
RSA - Generar Fichero de envío
DES - Generar Clave y Fichero
Insertar Fichero de Claves/Confirmación Remoto

A continuación aparece un dialogo donde se podrá indicar el path del fichero de intercambio que se generará automáticamente:


Genración de Fichero de intercambio de Claves
Se va a generar un fichero que contiene, la clave DES cifrada mediante una clave RSA.
El fichero generado deberá ser Enviado al Remoto y éste deberá insertarlo en su sistema para incorporar su clave DES.
Seleccione el nombre y el path del fichero a generar:
C:\gcdoc\D0000099950T1.txt
Defecto
Generar
Cancel

Si el subsistema está asociado con un Aplicación de EDItran/G entonces el fichero se enviará automáticamente por EDItran (ver sección **4.1.1.3**).

Ahora podremos comprobar que existen varias versiones:

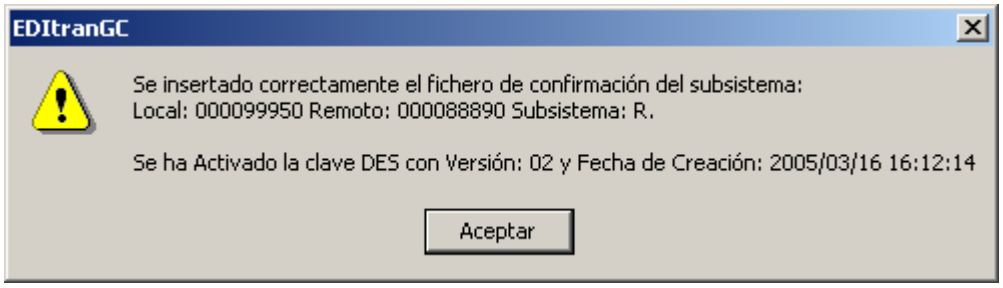


Se pueden almacenar hasta tres versiones de una clave y la lista muestra las versiones que se están almacenando en ese momento. Vemos que en la primera clave se almacena la versión 1 y que en la segunda la versión 2 y la tercera la versión 3. Además vemos que la versión 1 tiene una 'O' entre paréntesis indicando que está Operativa, la versión 2 una 'A' indicando que es la clave Activa y la versión 3 una 'S' indicando que se ha enviado el fichero de intercambio.

4.1.3. Inserción de un fichero de confirmación

Una vez que el remoto haya insertado nuestra clave DES, nos enviará un fichero de confirmación. Este fichero nos indica que el remoto incorporó la clave correctamente y así podemos nosotros activar la clave para que pueda ser utilizada con ese remoto.

Si estamos utilizando EDItran y tenemos el automatismo posterior a recepción de EDItran/GC, entonces al recibir la confirmación, automáticamente se activará la clave. Si no es así, entonces tendremos que insertar el fichero de confirmación pulsando sobre el botón "Inserción de fichero de Claves/Confirmación" de la barra de herramientas (ver apartado **2.3.7**). Aparecerá un dialogo indicando los datos de la confirmación:


EDItranGC
Se insertado correctamente el fichero de confirmación del subsistema:
Local: 000099950 Remoto: 000088890 Subsistema: R.
Se ha Activado la clave DES con Versión: 02 y Fecha de Creación: 2005/03/16 16:12:14
Aceptar

Ahora ya se dispone de una versión de la clave *"Activa"* para ese subsistema con ese remoto.

4.2. Creación de Subsistema Remoto DES

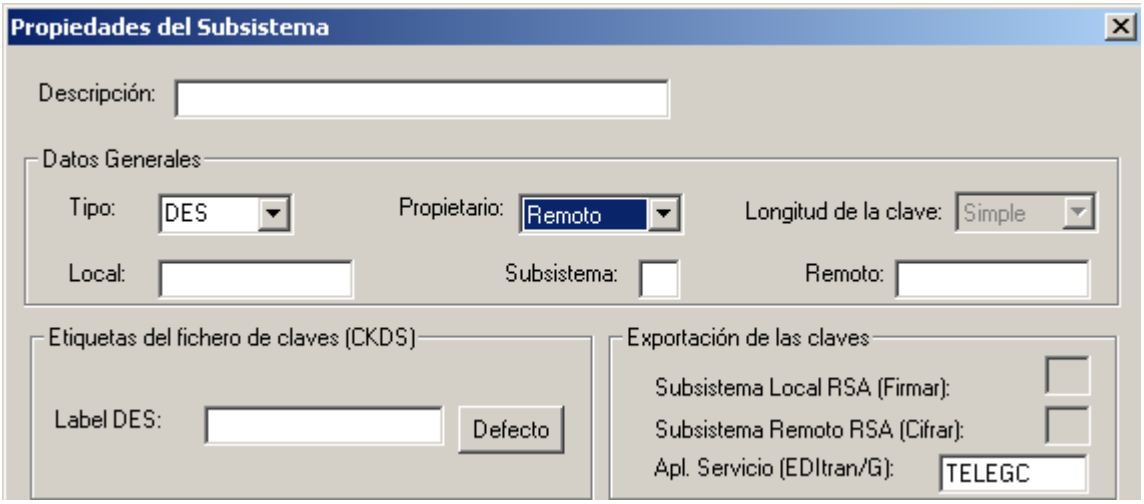
Se puede generar un subsistema remoto DES de tres formas, dos manuales y una automática:

- Automáticamente utilizando el programa de usuario de EDItran/G posterior a recepción (mirar sección XXXXXXXXXXXXXXXXXXX)
- Manualmente a través de la interfaz gráfica pinchando sobre el botón de la barra de herramientas *"Nuevo Subsistema"*.
- Manualmente a través de la interfaz gráfica pinchando sobre el botón de la barra de herramientas *"Inserción de fichero remoto"*.

En este apartado veremos las dos maneras manuales de añadir un subsistema remoto DES.

4.2.1. Creación de un subsistema Remoto DES

Para generar un subsistema Remoto DES, pinchar sobre el botón "Crear un Subsistema" de la barra de herramientas (ver apartado **2.3.1**). Aparecerá el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**) , seleccionar Tipo a *"DES"* y Propietario a *"Remoto":*



Se rellenan los datos de código local, código remoto y subsistema, opcionalmente se rellena la Descripción y se pulsa defecto para obtener las labeles por defecto, de ésta manera se asegura que no haya ninguna label repetida.

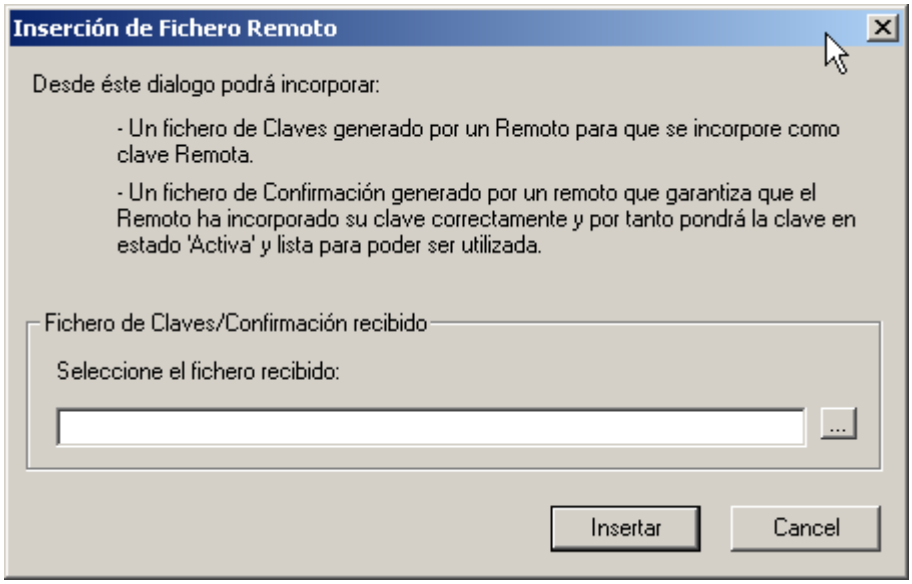
Por último se rellenan los datos de exportación de las claves. En Subsistema Local RSA habrá que poner un subsistema Local RSA asociado con el mismo remoto que el subsistema DES. Éste subsistema se utilizará para firmar los datos del fichero de intercambio. En Subsistema Remoto RSA se debe poner un subsistema Remoto RSA que nos haya enviado el mismo remoto que el dado de alta en el subsistema DES. Éste subsistema se utilizará para cifrar la clave que viajará en el fichero de intercambio.

La aplicación de servicio de EDItran/G se utiliza si se quiere enviar las confirmaciones por EDItran. Se recomienda utilizar la Aplicación de EDItran/G TELEG.

Pulsando sobre el botón *"OK"*, se generará un nuevo subsistema remoto DES. Sin embargo aún no se tiene la clave DES del remoto. Está se tendrá que añadir manualmente como se explica en el apartado siguiente o automáticamente mediante los automatismos de EDItran/G.

4.2.2. Incorporación de un fichero de intercambio remoto

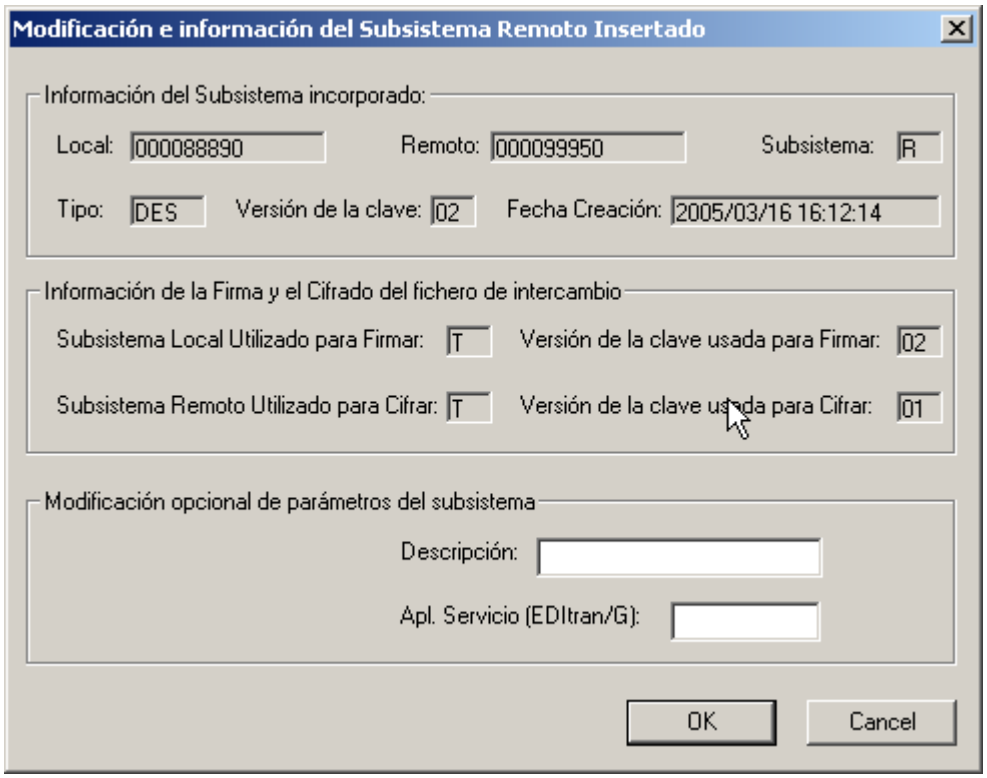
Al pinchar sobre el botón *"Inserción de Fichero Remoto"* aparecerá el dialogo:


Inserción de Fichero Remoto
Desde éste dialogo podrá incorporar:
- Un fichero de Claves generado por un Remoto para que se incorpore como clave Remota.
- Un fichero de Confirmación generado por un remoto que garantiza que el Remoto ha incorporado su clave correctamente y por tanto pondrá la clave en estado 'Activa' y lista para poder ser utilizada.
Fichero de Claves/Confirmación recibido
Seleccione el fichero recibido:
...
Insertar
Cancel

Se debe seleccionar el fichero de intercambio recibido por el remoto y pulsar Insertar.

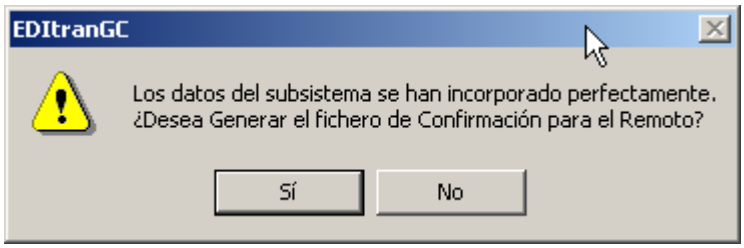
EDItran/GC primero comprueba la firma del fichero de intercambio, luego, si el subsistema que viene en el fichero no ha sido de alta previamente (como se indica en el apartado **4.2.1**) se genera automáticamente con los datos del fichero y por último se intenta descifrar la clave DES del remoto y si se logra ésta se incorpora en el fichero de claves de EDItran (ckds.des).

Una vez finalizado el proceso, aparece un dialogo mostrando la clave del subsistema que ha incorporado:


Modificación e información del Subsistema Remoto Insertado
Información del Subsistema incorporado:
Local: 000088890
Remoto: 000099950
Subsistema: R
Tipo: DES
Versión de la clave: 02
Fecha Creación: 2005/03/16 16:12:14
Información de la Firma y el Cifrado del fichero de intercambio
Subsistema Local Utilizado para Firmar: T
Versión de la clave usada para Firmar: 02
Subsistema Remoto Utilizado para Cifrar: T
Versión de la clave usada para Cifrar: 01
Modificación opcional de parámetros del subsistema
Descripción:
Apl. Servicio (EDItran/G):
OK
Cancel

En el dialogo de *Modificación e información del Subsistema Remoto Insertado*, aparecen dos campos para introducir, de forma opcional, una descripción del subsistema generado y la Aplicación de servicio por la que viajará el fichero de confirmación, si se tiene instalado EDItran (se recomienda utilizar TELEGC).

Al pulsar sobre el botón *"OK"* se nos da la opción de generar el fichero de confirmación:

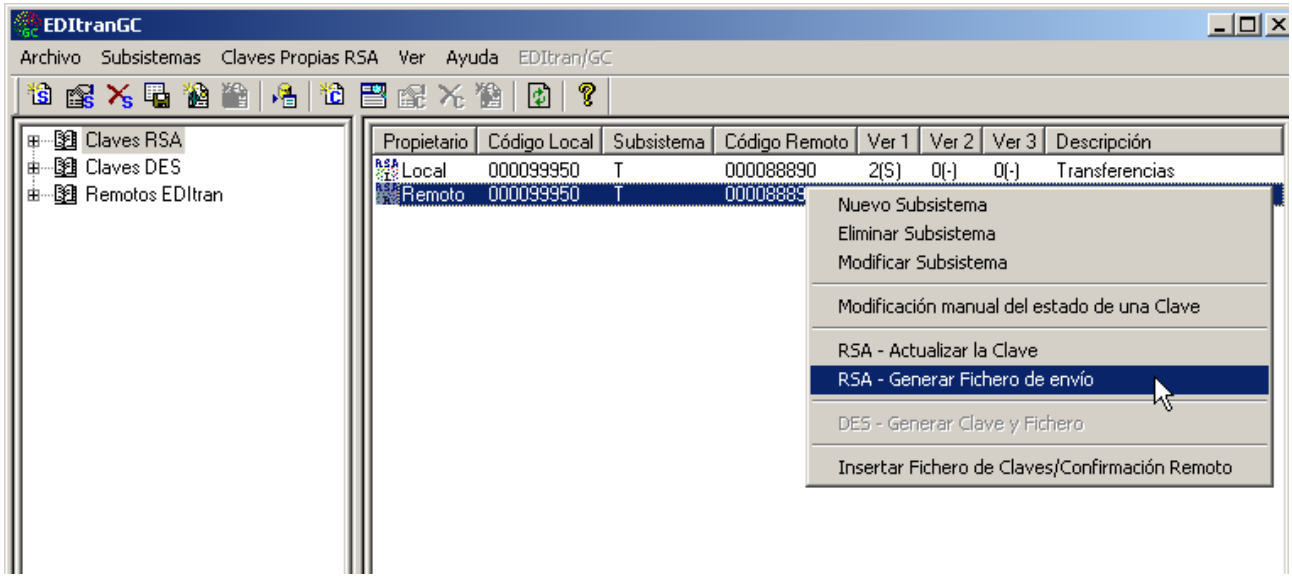

EDItranGC
Los datos del subsistema se han incorporado perfectamente.
¿Desea Generar el fichero de Confirmación para el Remoto?
Sí
No

Si pulsamos "Si" se genera el fichero de confirmación. No es obligatorio generar el fichero de confirmación en éste momento ya que lo podremos generar en otro momento posterior, sin embargo es recomendable generar el fichero en éste momento.

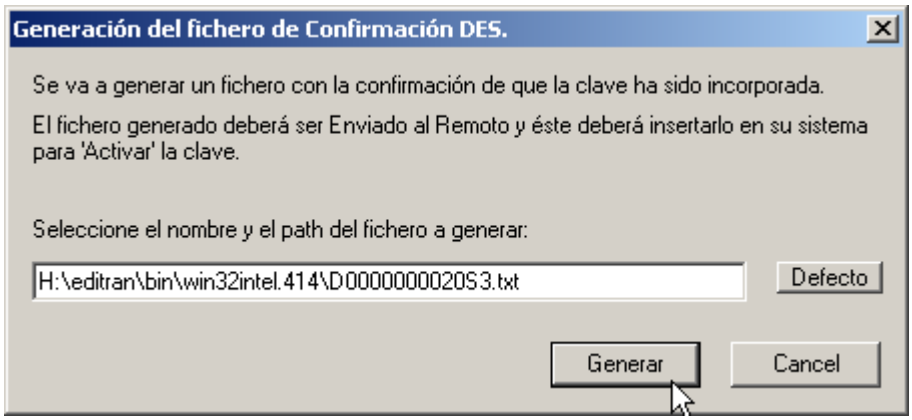
4.2.3. Generación y envío de la confirmación

Al incorporar una clave DES remota, se debe generar un fichero de confirmación que se enviará al remoto para que éste pueda comprobar que el proceso de incorporación se ha efectuado correctamente y así pasar la clave a estado *"Activa"* para que pueda ser utilizada por EDItran.

Como se ha indicado antes la confirmación se puede generar en el momento de inserción de la clave DES del remoto. Pero también se puede generar (de no haberse generado antes) en cualquier momento. Para eso se selecciona el subsistema remoto DES que se quiera confirmar, pinchando con el botón derecho y escogiendo *"RSA - Generar Fichero de envío":*


EDItranGC
Archivo Subsistemas Claves Propias RSA Ver Ayuda EDItran/GC
Claves RSA
Claves DES
Remotos EDItran
Propietario Código Local Subsistema Código Remoto Ver 1 Ver 2 Ver 3 Descripción
Local 000099950 T 000088890 2(S) 0(-) 0(-) Transferencias
Remoto 000099950 T
Nuevo Subsistema
Eliminar Subsistema
Modificar Subsistema
Modificación manual del estado de una Clave
RSA - Actualizar la Clave
RSA - Generar Fichero de envío
DES - Generar Clave y Fichero
Insertar Fichero de Claves/Confirmación Remoto

Tanto de manera automática (al insertar la clave) como de manera manual (en cualquier momento posterior como se acaba de indicar), aparece un dialogo donde se puede indicar el path del fichero de confirmación que se generará:


Generación del fichero de Confirmación DES.
Se va a generar un fichero con la confirmación de que la clave ha sido incorporada.
El fichero generado deberá ser Enviado al Remoto y éste deberá insertarlo en su sistema para 'Activar' la clave.
Seleccione el nombre y el path del fichero a generar:
H:\editran\bin\win32intel.414\D000000002053.txt
Defecto
Generar
Cancel

Si el subsistema tiene una Aplicación de Servicio de EDItran/G (típicamente será 'TELEG'), se intentará enviar el fichero por EDItran como se indica en el apartado **4.1.1.3**. Una vez generado el fichero y enviado por EDItran, se activará ésta versión de la clave, asegurándonos el intercambio seguro de ficheros con la versión de la última clave generada.

4.3. Otras operaciones comunes de subsistemas DES

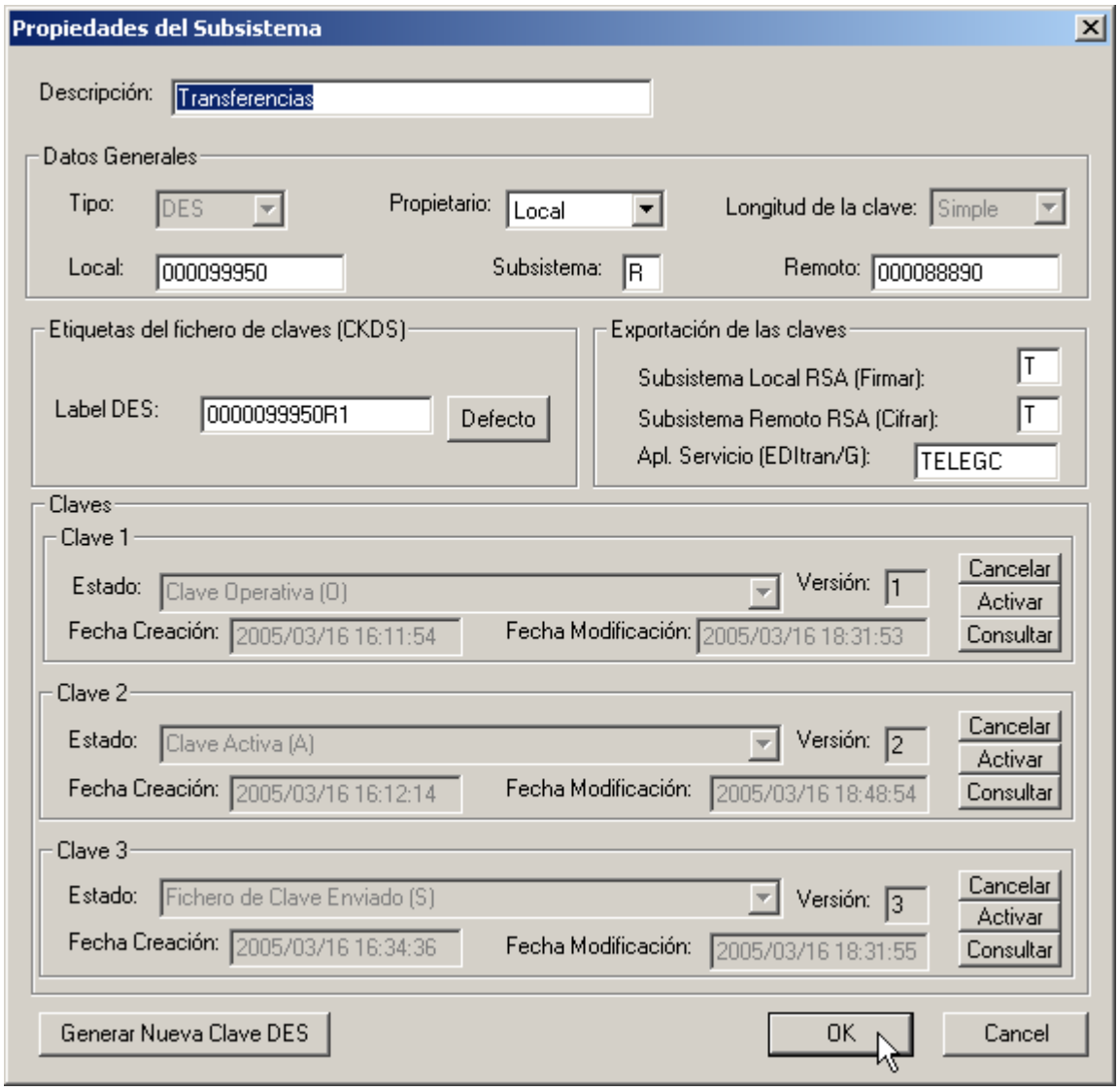
A continuación se detallarán funcionalidades comunes de los subsistemas Locales y Remotos DES.

4.3.1. Modificación, Consulta y Eliminación de un subsistema DES

Para ver todas los subsistemas locales de DES podemos selecciona en el árbol la rama adecuada (ver apartado **0**).

Para Eliminar un subsistema, seleccionarlo de la lista y pulsar <Del> o <Supr>.

Para Modificar o Consultar un subsistema, hacer doble clic sobre la línea de la lista. Aparece el dialogo de *Propiedades del Subsistema*:



Desde aquí se pueden realizar las siguientes operaciones:

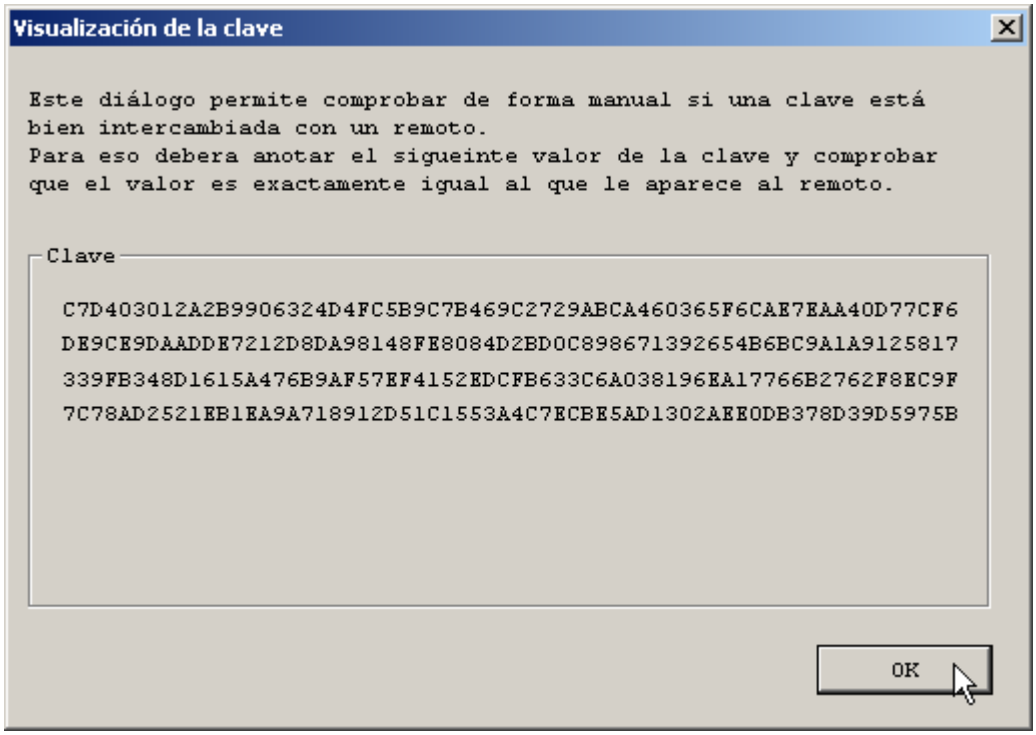
- Cambio de propiedades y ***modificación del subsistema***, pulsando el botón *"OK"*
- ***Consultar una versión de la clave***, pulsando sobre el botón *"Consultar"* de la versión de la clave (ver apartado **4.3.2**)
- ***Activar una versión de la clav***e, pulsando sobre el botón *"Activar"* de la versión de la clave que se desee activar (ver apartado **4.3.4**).

- ***Cancelar una versión de la clave***, pulsando sobre el botón *"Cancelar"* de la versión de la clave que se desee cancelar (ver apartado **4.3.4**).
- ***Generar una nueva versión de la clave DES***, pulsando sobre el botón *"Generar Nueva Clave DES"* se generará una nueva clave DES que se almacenará como una nueva versión de la clave del subsistema (ver apartado **4.1.2**).

4.3.2. Consulta de claves DES

Al pulsar sobre el botón *Consultar* de una versión del dialogo de *Propiedades del Subsistema* (ver apartado **4.3.1**) se podrá ver una *sello de la clave*. No es posible, por motivos de seguridad, mostrar directamente una clave DES. En lugar de eso se relaiza una serie de cifrados y descifrados de datos que dan lugar a lo que denominamos *sello de la clave*.

El siguiente dialogo muestra el resultado del *sello de la clave* DES:


Visualización de la clave
Este diálogo permite comprobar de forma manual si una clave está bien intercambiada con un remoto.
Para eso debera anotar el sigueinte valor de la clave y comprobar que el valor es exactamente igual al que le aparece al remoto.
Clave
C7D403012A2B9906324D4FC5B9C7B469C2729ABCA460365F6CAE7EAA40D77CF6
DE9CE9DAADDE7212D8DA98148FE8084D2BD0C898671392654B6BC9A1A9125817
339FB348D1615A476B9AF57EF4152EDCFB633C6A038196EA17766B2762F8EC9F
7C78AD2521EB1EA9A71891ZD51C1553A4C7ECBE5AD1302AEE0DB378D39D5975B
OK

Esta funcionalidad es útil para comparar que la clave local DES propia, que hemos generado y permanece en nuestro sistema, es idéntica a la que el remoto tiene incorporada en su sistema.

4.3.3. Modificación manual del estado de una clave DES

La modificación manual del estado de una clave puede ser una operación peligrosa ya que puede dejar inestable el subsistema al que se realice el cambio.

Sin embargo, en algunos casos, puede ser útil modificar manualmente el estado en que se encuentra alguna clave. Por ejemplo:

- Se ha enviado el fichero de intercambio con una clave DES pero el remoto no lo ha podido incorporar y se ha eliminado fichero. En esta circunstancia hay que crear de nuevo el fichero de intercambio modificando el estado de la versión de la clave a *"Clave Generada (G)"*.
- Ha habido un error al enviar el fichero por EDItran y el estado se ha quedado en *"Error al Enviar Fichero de Clave (E)"* o *"Error al Enviar Fichero de Confirmación (E)"* sin embargo se ha solucionado el problema el problema y el fichero se ha enviado

manualmente por EDItran. Entonces habrá que modificar el estado a *"Fichero de Claves Enviado (E)"* o *"Fichero de Confirmación Enviado(S)"* respectivamente.

Es recomendable no modificar manualmente el estado de una clave si no se conocen perfectamente el efecto que la modificación puede producir.

4.3.4. Activación y Cancelación de una clave DES

Mediante el dialogo de *Propiedades del Subsistema* (ver apartado **4.3.1**) se puede activar o cancelar una versión de una clave del subsistema.

Sólo puede haber una versión de una clave en estado *"Activa (A)"* en un subsistema. Cuando se activa una clave, ya sea automáticamente o manualmente, si otra clave estaba antes *"Activa (A)"*, entonces pasará a estado *"Operativa (O)"*. Para activar una versión de la clave, se debe pulsar el botón *"Activar"* de el dialogo de *Propiedades del Subsistema* (ver apartado **3.3.1**).

También se puede cancelar una versión de una clave. Cancelando la clave se asegura que la clave no pueda ser utilizada. Para cancelar una versión de la clave, se debe pulsar el botón *"Cancelar"* de el dialogo de *Propiedades del Subsistema* (ver apartado **4.3.1**).

5. Utilización de EDItran junto a EDItran/GC

La utilización de EDItran como medio de transmisión del fichero de intercambio facilita enormemente la operativa necesaria de EDItran/GC. Por tanto aunque no es obligatorio, es sumamente recomendable que EDItran/GC y EDItran estén instalados.

Fundamentalmente existen dos ventajas claves a la hora de tener instalado EDItran:

1. Posibilidad de envío y recepción automática desde la interfaz de EDItran/GC de los ficheros de confirmación y claves.
2. Posibilidad de incorporación automática desde EDItran, mediante un procedimiento de usuario posterior a recepción, del fichero de intercambio o del fichero de confirmación recibido.

A continuación se explicará cómo aprovechar cada una de las ventajas mencionadas.

5.1. Envío y recepción automática utilizando EDItran

5.1.1. Subsistema Local

Para que un fichero de intercambio que contenga una clave (ya sea RSA o DES), es decir un fichero generado por EDItran/GC al crear una nueva versión de una clave en un subsistema local, sea enviado automáticamente simplemente hay que añadir el parámetro de *Aplicación Servicio EDItran/G*.

Además habrá que dar de alta en EDItran/G la presentación, teniendo en cuenta que el código local y el código remoto de EDItran/G deben coincidir con el código local y el código remoto del subsistema de EDItran/GC.

5.1.2. Subsistema Remoto

Para que un fichero de confirmación (ya sea de un subsistema RSA o DES), es decir un fichero generado por EDItran/GC al insertar una nueva versión de una clave en un subsistema remoto, sea enviado automáticamente simplemente hay que añadir el parámetro de *Aplicación Servicio EDItran/G* en el subsistema Remoto.

Cuando se incorpora una clave de un subsistema remoto, se da la opción de añadir el parámetro *Aplicación Servicio EDItran/G*, consultar el apartado **3.2.2** para el caso de RSA y el apartado **4.2.2** para el caso DES.

Además habrá que dar de alta en EDItran/G la presentación, teniendo en cuenta que el código local y el código remoto de EDItran/G deben coincidir con el código local y el código remoto del subsistema de EDItran/GC.

5.1.3. Perfiles de EDItran/G

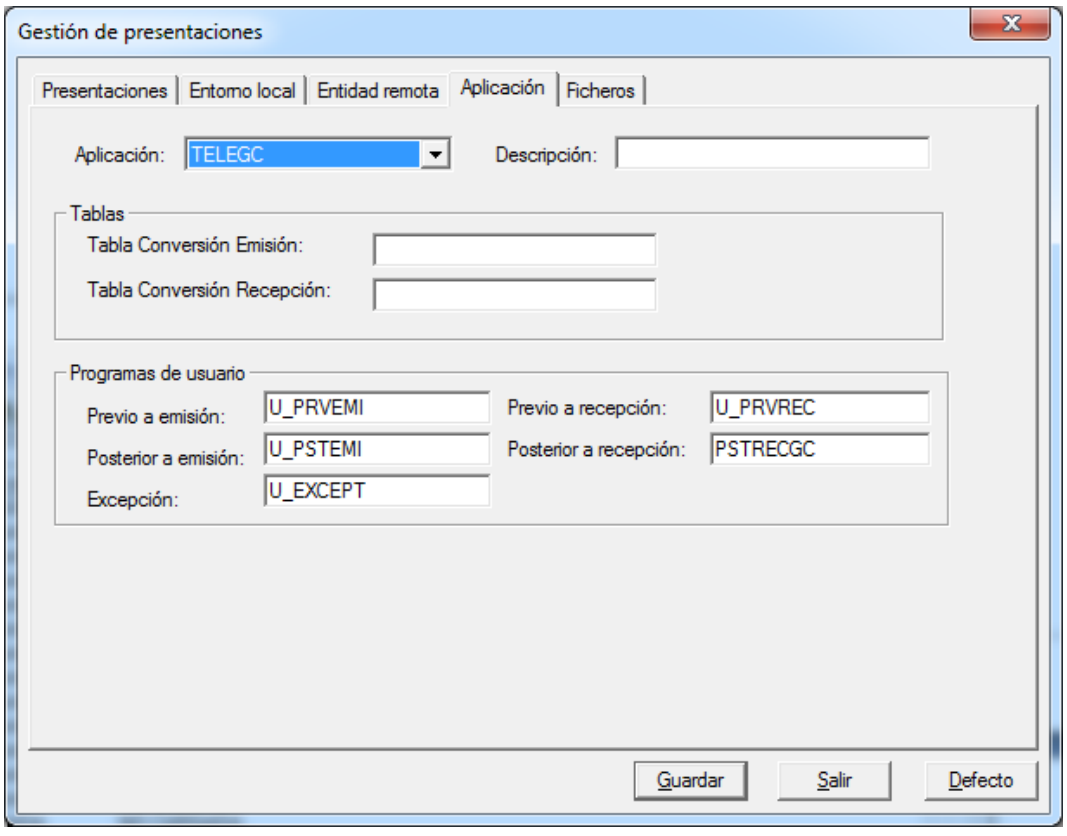
Los fichero de intercambio a trasmitir, tanto el fichero de claves RSA como el fichero de claves DES como el fichero confirmación tienen el mismo formato que habrá que dar de alta en las Presentaciones de EDItran/G. A continuación se añade una tabla donde aparecen los parámetros de configuración de la Presentación:

Sentido	Concepto	Valor
Emisión	Compresión	Si
Emisión	Alfabeto	ASCII
Emisión	Formato de Ficheros de Aplicación	Fijo
Emisión	Traducción ASCII/EBCDIC	No
Emisión	Longitud de registros de Aplicación	00823
Emisión	Delimitador	Ninguno
Recepción	Traducir en recepción	ASCII

5.2. Procedimiento Automático para EDItran

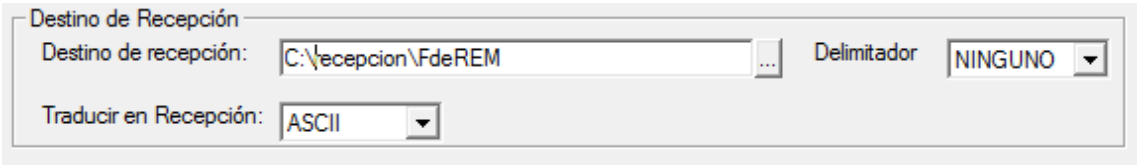
La segunda ventaja es la incorporación automática de los ficheros de intercambio de claves y de confirmación que el remoto nos envíe.

EDItran tiene la posibilidad de añadir programas de usuario que se ejecutan antes y después de las transmisiones. Si se quiere utilizar la incorporación automática de los ficheros, se deberá modificar el programa de usuario *"Posterior a recepción"* y poner el posterior a recepción de Editran/GC:



Por tanto de la Presentación de EDItran/G, con código local y código remoto igual que la dada de alta en EDItran/GC, y con la Aplicación de EDItran/G igual que la de EDItran/GC (es recomendable que se llame *'TELEGC'*) se deberá modificar el programa posterior a recepción U_PSTREC por PSTRECGC (puede que en su instalación se llame de otras manera).

Además es conveniente poner el como destino de recepción un nombre de un fichero en vez de un directorio. De esta manera nos aseguramos que el fichero que se recibe se llama siempre de la misma manera e igual a como se le ha dado de alta:



5.2.1. PSTRECGC.bat

El siguiente listado muestra el contenido del programa de usuario posterior a recepción de EDItran/GC (PSTRECGC.bat):

```
@echo off
rem
rem Automatismos de demostracion de EDItran/G.
rem
rem Comunicaciones (C) INDRA, Julio 2007.
rem
echo ################################################################################
echo SCRIPT DE USUARIO POSTERIOR A RECEPCION EDItran/GC: %0.
timestamp
echo PRESENTACION : %2-%1 (%4-%5-%6)
echo RESULTADO    : %2-%3
echo ################################################################################
sleep 10
insertgc -f FdeBESP -c
```

En la última línea del posterior a recepción está la llamada al comando *insertgc.exe* de Editran/GC. El segundo parámetro que se le pasa es el fichero que se ha recibido. Se deberá modificar el programa de usuario (PSTRECGC.bat) para que el segundo parámetro en la llamada a insertgc sea el fichero que se ha recibido.

El parámetro *-a* indica la aplicación de servicio de EDItran/GC. Este parámetro se utilizará únicamente cuando se vaya a incorporar automáticamente un nuevo subsistema remoto. En este caso el subsistema que se genere llevará como Aplicación de Servicio la misma Aplicación por la que se ha recibido el fichero. En los demás casos el parámetro se ignorará.

6. Apendices

6.1. Estados de los subsistemas

A continuación aparece una lista con todos los estados posibles de las claves de los subsistema:

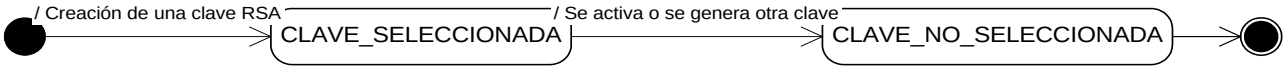
Id	Estado	Texto
1	CLAVE_GENERADA	Clave Generada
2	CLAVE_OPERATIVA	Clave Operativa
3	CLAVE_ACTIVA	Clave Activa
4	GENERADO_FICHERO_ENVIO_CLAVE	Generado el Fichero de Envió de Clave
5	ENVIANDO_FICHERO_CLAVE	Enviando el Fichero de Clave
6	ERROR_ENVIO_FICHERO_CLAVE	Error al Enviar el Fichero de Clave
7	FICHERO_CLAVE_ENVIADO	Fichero de Clave Enviado
8	RECIBIDA_CONFIRMACION	Confirmación Recibida
9	CONFIRMACION_INVALIDA	Recibido un Fichero de Confirmación Inválido
10	CLAVE_REMOTA_INSERTADA	Clave Remota Insertada
11	GENERADO_FICHERO_CONFIRMACION	Generado Fichero de Confirmación
12	ENVIANDO_FICHERO_CONFIRMACION	Enviando del Fichero de Confirmación
13	ERROR_ENVIO_FICHERO_CONFIRMACION	Error al Enviar el Fichero de Confirmación
14	FICHERO_CONFIRMACION_ENVIADO	Fichero de Confirmación Enviado
15	CLAVE_CANCELADA	Clave Cancelada
16	CLAVE_NO_SELECCIONADA	Clave NO Seleccionada
17	CLAVE_SELECCIONADA	Clave Seleccionada

La tabla será útil para localizar por el identificador cada uno de los estados del siguiente diagrama.

6.2. Diagrama de Estados

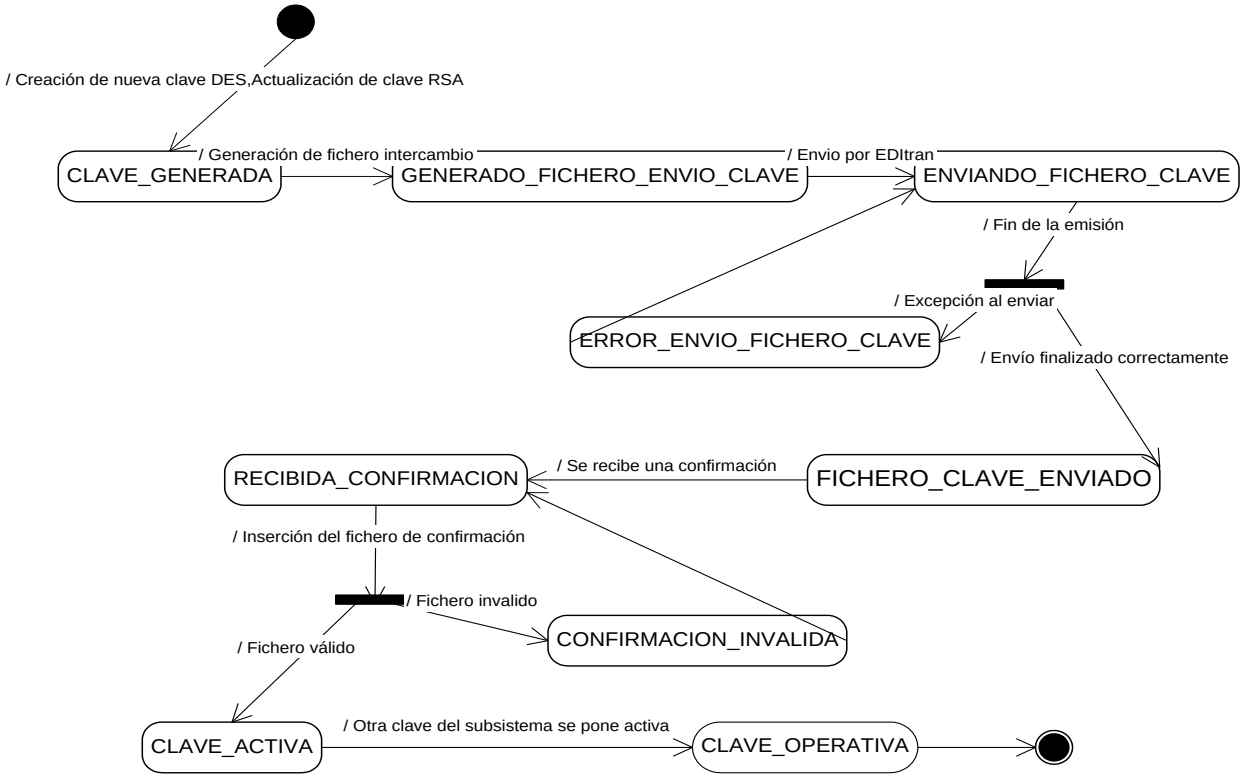
6.2.1. Clave Propia RSA

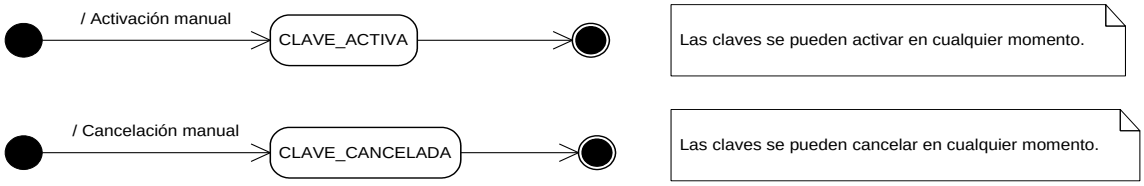
Diagrama de secuencia de estados para una clave de un Subsistema propio RSA:



6.2.2. Clave Local

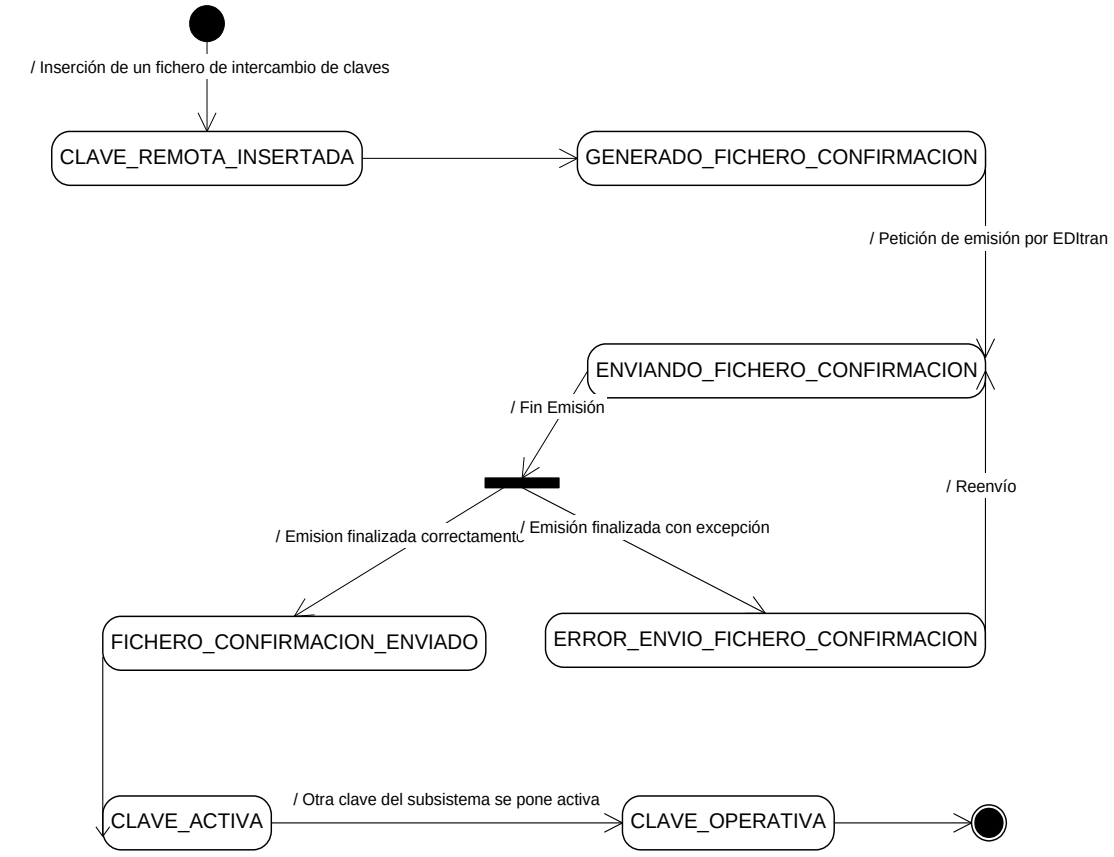
Diagrama de secuencia de estados para una clave Local tanto RSA como DES:

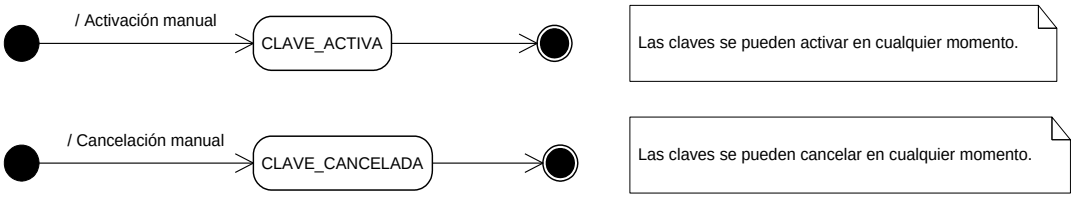



/ Activación manual
CLAVE_ACTIVA
Las claves se pueden activar en cualquier momento.
/ Cancelación manual
CLAVE_CANCELADA
Las claves se pueden cancelar en cualquier momento.

6.2.3. Clave Remota

Diagrama de secuencia de estados para una clave Remota tanto RSA como DES:




/ Activación manual
CLAVE_ACTIVA
Las claves se pueden activar en cualquier momento.
/ Cancelación manual
CLAVE_CANCELADA
Las claves se pueden cancelar en cualquier momento.

Centros de Competencia eCommerce

Avda. de Bruselas 35
28108 Alcobendas.
Madrid, España
T. +34 91 480 80 80
T. +34 91 480 50 00
www.indracompany.com